3Com Switch 4500 Family

Configuration Guide

Switch 4500 26-Port

Switch 4500 50-Port

Switch 4500 PWR 26-Port

Switch 4500 PWR 50-Port

Product Version: V03.03.00
Manual Version:
6W101-20090811
www.3com.com

3Com Corporation
350 Campus Drive, Marlborough,
MA, USA 01752 3064

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

About This Manual

Organization

3Com Switch 4500 Family Configuration Guide is organized as follows:

Part	Contents
1 Login	Introduces the ways to log into an Ethernet switch and CLI related configuration.
2 Configuration File Management	Introduces configuration file and the related configuration.
3 VLAN	Introduces VLAN and related configuration.
4 IP Address and Performance Optimization	Introduces IP address and IP performance optimization related configuration
5 Voice VLAN	Introduces voice VLAN and the related configuration.
6 Port Basic Configuration	Introduces port basic configuration.
7 Link Aggregation	Introduces link aggregation and the related configuration.
8 Port Isolation	Introduces port isolation and the related configuration.
9 Port Security	Introduces port security and the related configuration.
10 DLDP	Introduces DLDP and the related configuration.
11 MAC Address Table Management	Introduces MAC address forwarding table management and the related configuration
12 Auto Detect	Introduces auto detect function and the related configuration.
13 MSTP	Introduces STP, MSTP, and the related configuration.
14 Routing Protocol	Introduces static routing protocol, RIP, routing policy, and the related configuration.
15 Multicast	Introduces multicast, IGMP snooping, and the related configuration.
16 802.1x and System Guard	Introduces 802.1x and the related configuration.
17 AAA	Introduces AAA, RADIUS, EAD, and the related configurations.
18 MAC Address Authentication	Introduces MAC address authentication and the related configuration.
19 ARP	Introduces ARP and the related configuration.
20 DHCP	Introduces DHCP relay agent, DHCP Snooping, DHCP/BOOTP client, and the related configuration.
21 ACL	Introduces ACL and the related configuration.
22 QoS	Introduces QoS and the related configuration.
23 Mirroring	Introduces mirroring and the related configuration.
24 XRN Fabric	Introduces XRN fabric and the related configuration.
25 Cluster	Introduces cluster and the related configuration.
26 PoE-PoE Profile	Introduces PoE, PoE profile and the related configuration.

Part	Contents
27 UDP Helper	Introduces UDP helper and the related configuration.
28 SNMP-RMON	Introduces the configuration for network management through SNMP and RMON
29 NTP	Introduces NTP and the related configuration.
30 SSH	Introduces SSH2.0 and the related configuration.
31 File System Management	Introduces basic configuration for file system management.
32 FTP-SFTP-TFTP	Introduces basic configuration for FTP, SFTP and TFTP, and the applications.
33 Information Center	Introduces information center and the related configuration.
34 System Maintenance and Debugging	Introduces system maintenance and debugging.
35 VLAN-VPN	Introduces VLAN-VPN, selective QinQ, and the related configuration.
36 Remote-ping	Introduces Remote-ping and the related configuration.
37 IPv6 Management	Introduces IPv6, IPv6 applications, and the related configuration.
38 Access Management	Introduces Access Management and the related configuration.
39 Appendix	Lists the acronyms used in this manual

Conventions

The manual uses the following conventions:

Command conventions

<table>
<tr><th>Convention</th><th>Description</th></tr>
<tr><td>Boldface</td><td>The keywords of a command line are in Boldface.</td></tr>
<tr><td>italic</td><td>Command arguments are in italic.</td></tr>
<tr><td>[ ]</td><td>Items (keywords or arguments) in square brackets [ ] are optional.</td></tr>
<tr><td>{ x | y | ... }</td><td>Alternative items are grouped in braces and separated by vertical bars. One is selected.</td></tr>
<tr><td>[x | y | ...]</td><td>Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.</td></tr>
<tr><td>{ x | y | ... } *</td><td>Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.</td></tr>
<tr><td>[x | y | ...] *</td><td>Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.</td></tr>
<tr><td>&<1-n></td><td>The argument(s) before the ampersand (&) sign can be entered 1 to n times.</td></tr>
<tr><td>#</td><td>A line starting with the # sign is comments.</td></tr>
</table>

GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click <OK>.
[ ]	Window names, menu items, data table and field names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

Symbols

Convention	Description
Warning	Means reader be extremely careful. Improper operation may cause bodily injury.
Caution	Means reader be careful. Improper operation may cause data loss or damage to equipment.
Note	Means a complementary description.

Related Documentation

In addition to this manual, each 3com Switch 4500 documentation set includes the following:

Manual	Description
3Com Switch 4500 Family Command Reference Guide	Provide detailed descriptions of command line interface (CLI) commands, that you require to manage your switch.
3Com Switch 4500 Family Quick Reference Guide	Provide a summary of command line interface (CLI) commands that are required for you to manage your Stackable Switch.
3Com Switch 4500 Family Getting Started Guide	This guide provides all the information you need to install and use the 3Com Switch 4500 Family.
3Com Switch 4500 Family Release Notes	Contain the latest information about your product. If information in this guide differs from information in the release notes, use the information in the Release Notes.

Obtaining Documentation

You can access the most up-to-date 3Com product documentation on the World Wide Web at this URL: http://www.3com.com.

Table of Contents

1 Logging In to an Ethernet Switch

Go to these sections for information you are interested in:

- Logging In to an Ethernet Switch
- Introduction to the User Interface

Logging In to an Ethernet Switch

To manage or configure a Switch 4500, you can log in to it in one of the following three methods:

- Command Line Interface
- Web-based Network Management Interface
- Network Management Station

The following table shows the configurations corresponding to each method:

Method	Tasks
Command Line Interface	Logging In Through the Console Port
	Logging In Through Telnet
	Logging In Using a Modem
	CLI Configuration
Web-based Network Management Interface	Logging In Through the Web-based Network Management Interface
Network Management Station	Logging In Through NMS

Introduction to the User Interface

Supported User Interfaces

Note

The auxiliary (AUX) port and the console port of a 3Com low-end and mid-range Ethernet switch are the same port (referred to as console port in the following part). You will be in the AUX user interface if you log in through this port.

Switch 4500 supports two types of user interfaces: AUX and VTY.

- AUX user interface: A view when you log in through the AUX port. AUX port is a line device port.
- Virtual type terminal (VTY) user interface: A view when you log in through VTY. VTY port is a logical terminal line used when you access the device by means of Telnet or SSH.

Table 1-1 Description on user interface

User interface	Applicable user	Port used	Remarks
AUX	Users logging in through the console port	Console port	Each switch can accommodate one AUX user.
VTY	Telnet users and SSH users	Ethernet port	Each switch can accommodate up to five VTY users.

One user interface corresponds to one user interface view, where you can configure a set of parameters, such as whether to authenticate users at login and the user level after login. When the user logs in through a user interface, the connection follows these parameter settings, thus implementing centralized management of various sessions.

Relationship Between a User and a User Interface

You can monitor and manage users logging in through different modes by setting different types of user interfaces. Switch 4500 provides one AUX user interface and five VTY user interfaces.

- A user interface does not necessarily correspond to a specific user.
- When a user logs in, the system automatically assigns the user a free user interface with the smallest number based on the user login mode. The login process of the user is restricted by the configurations under this user interface.
- The user interface assigned to a user depending on the login mode and login time.

A user interface can be used by one user at one time, however, the user interface is not dedicated to a specific user. For example, user A can use VTY 0 to log in to the device. When user A logs out, user B can use VTY 0 to log in to the device.

User Interface Index

Two kinds of user interface index exist: absolute user interface index and relative user interface index.

1) The absolute user interface indexes are as follows:

- The absolute AUX user interfaces are numbered 0 through 7.
- VTY user interface indexes follow AUX user interface indexes. The first absolute VTY user interface is numbered 8, the second is 9, and so on.

2) A relative user interface index can be obtained by appending a number to the identifier of a user interface type. It is generated by user interface type. The relative user interface indexes are as follows:

- AUX user interfaces are numbered from AUX0 to AUX7.
- VTY user interfaces are numbered VTY0, VTY1, and so on.

Note

Switch 4500 supports XRN Fabric. A Fabric can contain up to eight devices. Accordingly, the AUX user interfaces in a Fabric can be numbered from AUX0 to AUX7, through which all the console ports of the units in a Fabric can be identified. Refer to the XRN Fabric part for information about Fabric.

Common User Interface Configuration

Follow these steps to configure common user interface:

To do…	Use the command…	Remarks
Lock the current user interface	**lock**	Optional Available in user view A user interface is not locked by default.
Specify to send messages to all user interfaces/a specified user interface	**send** { **all** | *number* | *type number* }	Optional Available in user view
Free a user interface	**free user-interface** [*type*] *number*	Optional Available in user view
Enter system view	**system-view**	—
Set the banner	**header** [**incoming** | **legal** | **login** | **shell**] *text*	Optional By default, no banner is configured
Set a system name for the switch	**sysname** *string*	Optional
Enable copyright information displaying	**copyright-info enable**	Optional By default, copyright displaying is enabled. That is, the copy right information is displayed on the terminal after a user logs in successfully.
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—
Display the information about the current user interface/all user interfaces	**display users** [**all**]	Optional Available in any view.
Display the physical attributes and configuration of the current/a specified user interface	**display user-interface** [*type number* | *number*]	
Display the information about the current web users	**display web users**	

2 Logging In Through the Console Port

Go to these sections for information you are interested in:

- Introduction
- Setting Up a Login Environment for Login Through the Console Port
- Console Port Login Configuration
- Console Port Login Configuration with Authentication Mode Being None
- Console Port Login Configuration with Authentication Mode Being Password
- Console Port Login Configuration with Authentication Mode Being Scheme

Introduction

To log in through the console port is the most common way to log in to a switch. It is also the prerequisite to configure other login methods. By default, you can locally log in to Switch 4500 through its console port only.

Table 2-1 lists the default settings of a console port.

Table 2-1 The default settings of a console port

Setting	Default
Baud rate	19,200 bps
Flow control	None
Check mode (Parity)	None
Stop bits	1
Data bits	8

To log in to a switch through the console port, make sure the settings of both the console port and the user terminal are the same.

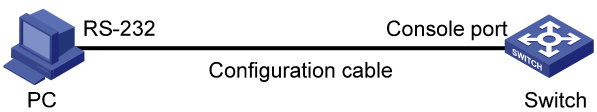
After logging in to a switch, you can perform configuration for AUX users. Refer to Console Port Login Configuration for more.

Setting Up a Login Environment for Login Through the Console Port

Following are the procedures to connect to a switch through the console port.

1) Connect the serial port of your PC/terminal to the console port of the switch, as shown in Figure 2-1.

Figure 2-1 Diagram for connecting to the console port of a switch

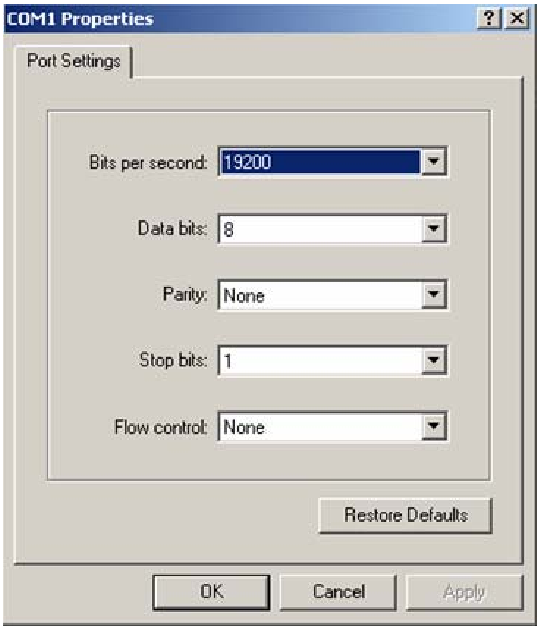


2) If you use a PC to connect to the console port, launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 9X/Windows 2000/Windows XP. The following assumes that you are running Windows XP) and perform the configuration shown in Figure 2-2 through Figure 2-4 for the connection to be created. Normally, both sides (that is, the serial port of the PC and the console port of the switch) are configured as those listed in Table 2-1.

Figure 2-2 Create a connection

Figure 2-3 Specify the port used to establish the connection

Figure 2-4 Set port parameters



3) Turn on the switch. You will be prompted to press the Enter key if the switch successfully completes POST (power-on self test). The prompt appears after you press the Enter key.

4) You can then configure the switch or check the information about the switch by executing the corresponding commands. You can also acquire help by typing the ? character. Refer to related parts in this manual for information about the commands used for configuring the switch.

Console Port Login Configuration

Common Configuration

Table 2-2 Common configuration of console port login

Configuration		Remarks
Console port configuration	Baud rate	Optional The default baud rate is 19,200 bps.
	Check mode	Optional By default, the check mode of the console port is set to “none”, which means no check bit.
	Stop bits	Optional The default stop bits of a console port is 1.
	Data bits	Optional The default data bits of a console port is 8.
AUX user interface configuration	Configure the command level available to the users logging in to the AUX user interface	Optional By default, commands of level 3 are available to the users logging in to the AUX user interface.
Terminal configuration	Make terminal services available	Optional By default, terminal services are available in all user interfaces

Configuration		Remarks
	Set the maximum number of lines the screen can contain	Optional By default, the screen can contain up to 24 lines.
	Set history command buffer size	Optional By default, the history command buffer can contain up to 10 commands.
	Set the timeout time of a user interface	Optional The default timeout time is 10 minutes.

Caution

The change to console port configuration takes effect immediately, so the connection may be disconnected when you log in through a console port and then configure this console port. To configure a console port, you are recommended to log in to the switch in other ways. To log in to a switch through its console port after you modify the console port settings, you need to modify the corresponding settings of the terminal emulation utility running on your PC accordingly in the dialog box shown in Figure 2-4.

Follow these steps to set common configuration of console port login:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enter AUX user interface view		**user-interface aux** 0	—
Configure the console port	Set the baud rate	**speed** *speed-value*	Optional The default baud rate of a console port is 19,200 bps.
	Set the check mode	**parity** { **even** | **none** | **odd** }	Optional By default, the check mode of a console port is **none**, that is, no check is performed.
	Set the stop bits	**stopbits** { **1** | **1.5** | **2** }	Optional The stop bits of a console port is 1.
	Set the databits	**databits** { **7** | **8** }	Optional The default databits of a console port is 8.
Configure the command level available to users logging in to the user interface		**user privilege level** *level*	Optional By default, commands of level 3 are available to users logging in to the AUX user interface, and commands of level 0 are available to users logging in to the VTY user interface.
Enable terminal services		**shell**	Optional By default, terminal services are available in all user interfaces.

To do…	Use the command…	Remarks
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.
Set the history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10, that is, a history command buffer of a user can store up to 10 commands by default.
Set the timeout time for the user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Console Port Login Configurations for Different Authentication Modes

Table 2-3 Console port login configurations for different authentication modes

Authentication mode	Authentication related configuration	Remarks
None	Set the authentication mode to none	Optional Refer to Console Port Login Configuration with Authentication Mode Being None
Password	Set the authentication mode to local password authentication	Refer to Console Port Login Configuration with Authentication Mode Being Password.
	Set the password for local authentication	
Scheme	Set the authentication mode to scheme	Refer to Console Port Login Configuration with Authentication Mode Being Scheme.
	Specify to perform local authentication or remote authentication	
	Set user names and passwords locally or on AAA Server	

Note

Changes made to the authentication mode for console port login takes effect after you quit the command-line interface and then log in again.

Console Port Login Configuration with Authentication Mode Being None

Configuration Procedure

Follow these steps to configure console port login with the authentication mode being none:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter AUX user interface view	**user-interface aux** 0	—
Configure not to authenticate users	**authentication-mode none**	Required By default, users logging in through the console port (AUX user interface) are not authenticated.

Configuration Example

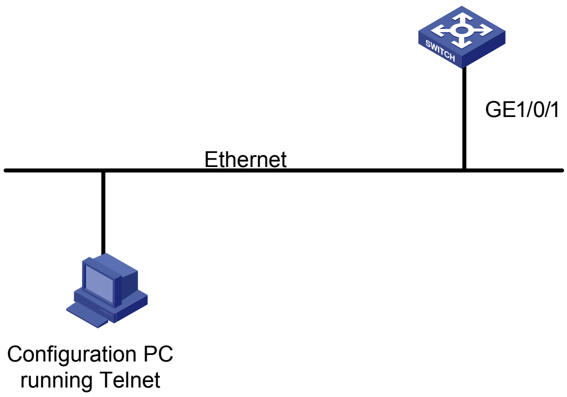
Network requirements

Assume that the switch is configured to allow users to log in through Telnet, and the current user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- Do not authenticate the users.
- Commands of level 2 are available to the users logging in to the AUX user interface.
- The baud rate of the console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

Network diagram

Figure 2-5 Network diagram for AUX user interface configuration (with the authentication mode being none)



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Enter AUX user interface view.

```
[Sysname] user-interface aux 0
```

Specify not to authenticate users logging in through the console port.

```
[Sysname-ui-aux0] authentication-mode none
```

Specify commands of level 2 are available to users logging in to the AUX user interface.

```
[Sysname-ui-aux0] user privilege level 2
```

Set the baud rate of the console port to 19,200 bps.

```
[Sysname-ui-aux0] speed 19200
```

Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-aux0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-aux0] history-command max-size 20
```

Set the timeout time of the AUX user interface to 6 minutes.

```
[Sysname-ui-aux0] idle-timeout 6
```

After the above configuration, you need to modify the configuration of the terminal emulation utility running on the PC accordingly in the dialog box shown in Figure 2-4 to log in to the switch successfully.

Console Port Login Configuration with Authentication Mode Being Password

Configuration Procedure

Follow these steps to configure console port login with the authentication mode being password:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter AUX user interface view	**user-interface aux** 0	—
Configure to authenticate users using the local password	**authentication-mode password**	Required By default, users logging in to a switch through the console port are not authenticated; while those logging in through Modems or Telnet are authenticated.
Set the local password	**set authentication password** { **cipher** | **simple** } *password*	Required

Configuration Example

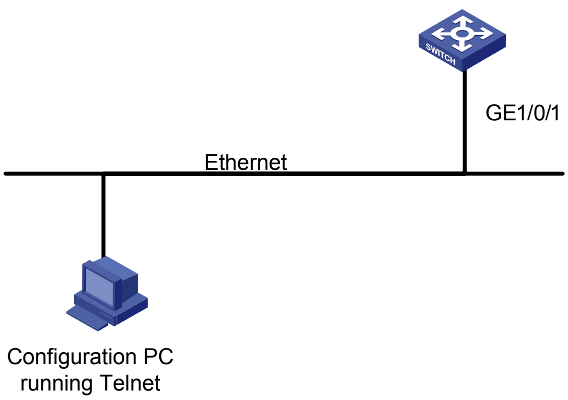
Network requirements

Assume the switch is configured to allow users to log in through Telnet, and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- Authenticate the users using passwords.
- Set the local password to 123456 (in plain text).
- The commands of level 2 are available to the users.
- The baud rate of the console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

Network diagram

Figure 2-6 Network diagram for AUX user interface configuration (with the authentication mode being password)



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Enter AUX user interface view.

```
[Sysname] user-interface aux 0
```

Specify to authenticate users logging in through the console port using the local password.

```
[Sysname-ui-aux0] authentication-mode password
```

Set the local password to 123456 (in plain text).

```
[Sysname-ui-aux0] set authentication password simple 123456
```

Specify commands of level 2 are available to users logging in to the AUX user interface.

```
[Sysname-ui-aux0] user privilege level 2
```

Set the baud rate of the console port to 19,200 bps.

```
[Sysname-ui-aux0] speed 19200
```

Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-aux0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-aux0] history-command max-size 20
```

Set the timeout time of the AUX user interface to 6 minutes.

```
[Sysname-ui-aux0] idle-timeout 6
```

After the above configuration, you need to modify the configuration of the terminal emulation utility running on the PC accordingly in the dialog box shown in Figure 2-4 to log in to the switch successfully.

Console Port Login Configuration with Authentication Mode Being Scheme

Configuration Procedure

Follow these steps to configure console port login with the authentication mode being scheme:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter AUX user interface view	**user-interface aux** 0	—
Configure to authenticate users in the scheme mode	**authentication-mode scheme** [**command-authorization**]	Required The specified AAA scheme determines what authentication mode is adopted, local or RADIUS. By default, users logging in through the console port (AUX user interface) are not authenticated.
Quit to system view	**quit**	—

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td rowspan="3">Configure the authentication mode</td><td>Enter the default ISP domain view</td><td>domain domain-name</td><td rowspan="3">Optional
By default, the local AAA scheme is applied.
If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well.
If you specify to apply a RADIUS scheme, you need to perform the following configuration as well:
• Perform RADIUS configuration on the switch. (Refer to the AAA part for more.)
• Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.)</td></tr>
<tr><td>Specify the AAA scheme to be applied to the domain</td><td>scheme { local | none | radius-scheme radius-scheme-name [local] }</td></tr>
<tr><td>Quit to system view</td><td>quit</td></tr>
<tr><td colspan="2">Create a local user (Enter local user view.)</td><td>local-user user-name</td><td>Required
No local user exists by default.</td></tr>
<tr><td colspan="2">Set the authentication password for the local user</td><td>password { simple | cipher } password</td><td>Required</td></tr>
<tr><td colspan="2">Specify the service type for AUX users</td><td>service-type terminal [level level]</td><td>Required</td></tr>
</table>

Note that:

If you configure to authenticate the users in the scheme mode, the command level available to users logging in to a switch depends on the command level specified in the AAA scheme:

- When the AAA scheme is local authentication, the command level available to users depends on the **service-type terminal** [**level** *level*] command.
- When the AAA scheme is RADIUS authentication, you need to set the corresponding user level on the RADIUS server.

Note

For the introduction to AAA, RADIUS, refer to the AAA part of this manual.

Configuration Example

Network requirements

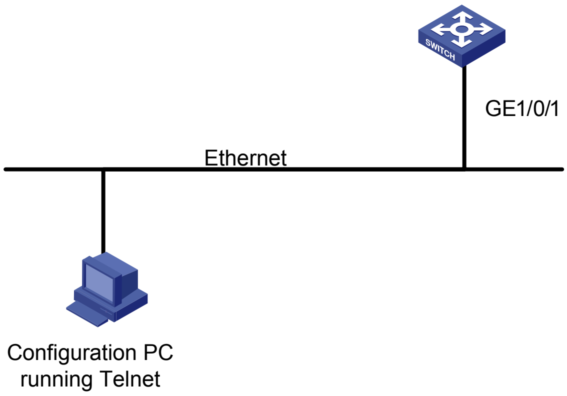
Assume the switch is configured to allow users to log in through Telnet, and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in through the console port (AUX user interface).

- Configure the local user name as **guest**.
- Set the authentication password of the local user to **123456** (in plain text).

- Set the service type of the local user to Terminal and the command level to 2.
- Configure to authenticate the users in the scheme mode.
- The baud rate of the console port is 19,200 bps.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of the AUX user interface is 6 minutes.

Network diagram

Figure 2-7 Network diagram for AUX user interface configuration (with the authentication mode being scheme)



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Create a local user named guest and enter local user view.

```
[Sysname] local-user guest
```

Set the authentication password to 123456 (in plain text).

```
[Sysname-luser-guest] password simple 123456
```

Set the service type to Terminal, Specify commands of level 2 are available to users logging in to the AUX user interface.

```
[Sysname-luser-guest] service-type terminal level 2
[Sysname-luser-guest] quit
```

Enter AUX user interface view.

```
[Sysname] user-interface aux 0
```

Configure to authenticate users logging in through the console port in the scheme mode.

```
[Sysname-ui-aux0] authentication-mode scheme
```

Set the baud rate of the console port to 19,200 bps.

```
[Sysname-ui-aux0] speed 19200
```

Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-aux0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-aux0] history-command max-size 20
```

Set the timeout time of the AUX user interface to 6 minutes.

```
[Sysname-ui-aux0] idle-timeout 6
```

After the above configuration, you need to modify the configuration of the terminal emulation utility running on the PC accordingly in the dialog box shown in Figure 2-4 to log in to the switch successfully.

3 Logging In Through Telnet

Go to these sections for information you are interested in:

- Introduction
- Telnet Configuration with Authentication Mode Being None
- Telnet Configuration with Authentication Mode Being Password

Introduction

Switch 4500 supports Telnet. You can manage and maintain a switch remotely by Telnetting to the switch.

To log in to a switch through Telnet, the corresponding configuration is required on both the switch and the Telnet terminal.

You can also log in to a switch through SSH. SSH is a secure shell added to Telnet. Refer to the *SSH Operation* for related information.

Table 3-1 Requirements for Telnetting to a switch

Item	Requirement
Switch	The IP address is configured for the VLAN of the switch, and the route between the switch and the Telnet terminal is reachable. (Refer to the *IP Address Configuration – IP Performance Configuration* and *Routing Protocol* parts for more.)
	The authentication mode and other settings are configured. Refer to Table 3-2 and Table 3-3.
Telnet terminal	Telnet is running.
	The IP address of the VLAN interface of the switch is available.

Note

Telnetting to a switch using IPv6 protocols is similar to Telnetting to a switch using IPv4 protocols. Refer to the *IPv6 Management* part for related information.

Common Configuration to Control Telnet Access

Table 3-2 Common Telnet configuration

Configuration		Description
VTY user interface configuration	Configure the command level available to users logging in to the VTY user interface	Optional By default, commands of level 0 are available to users logging in to a VTY user interface.

Configuration		Description
	Configure the protocols the user interface supports	Optional By default, Telnet and SSH protocol are supported.
	Set the commands to be executed automatically after a user log in to the user interface successfully	Optional By default, no command is executed automatically after a user logs into the VTY user interface.
VTY terminal configuration	Make terminal services available	Optional By default, terminal services are available in all user interfaces
	Set the maximum number of lines the screen can contain	Optional By default, the screen can contain up to 24 lines.
	Set history command buffer size	Optional By default, the history command buffer can contain up to 10 commands.
	Set the timeout time of a user interface	Optional The default timeout time is 10 minutes.

Follow these steps to set common telnet configuration:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	—
Configure the command level available to users logging in to VTY user interface	**user privilege level** *level*	Optional By default, commands of level 0 are available to users logging in to VTY user interfaces.
Configure the protocols to be supported by the VTY user interface	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional By default, both Telnet protocol and SSH protocol are supported.
Set the commands to be executed automatically after a user logs in to the user interface successfully	**auto-execute command** *text*	Optional By default, no command is executed automatically after a user logs into the VTY user interface.
Enable terminal services	**shell**	Optional By default, terminal services are available in all user interfaces.
Set the maximum number of lines the screen can contain	**screen-length** *screen-length*	Optional By default, the screen can contain up to 24 lines. You can use the **screen-length** 0 command to disable the function to display information in pages.

To do…	Use the command…	Remarks
Set the history command buffer size	**history-command max-size** *value*	Optional The default history command buffer size is 10, that is, the history command buffer of a user can store up to 10 commands by default.
Set the timeout time of the VTY user interface	**idle-timeout** *minutes* [*seconds*]	Optional The default timeout time of a user interface is 10 minutes. With the timeout time being 10 minutes, the connection to a user interface is terminated if no operation is performed in the user interface within 10 minutes. You can use the **idle-timeout** 0 command to disable the timeout function.

Telnet Configurations for Different Authentication Modes

Table 3-3 Telnet configurations for different authentication modes

Authentication mode	Authentication related configuration	Description
None	Set the authentication mode to none	Refer to Console Port Login Configuration with Authentication Mode Being None.
Password	Set the authentication mode to local password authentication	Refer to Console Port Login Configuration with Authentication Mode Being Password.
	Set the password for local authentication	
Scheme	Set the authentication mode to scheme	Refer to Console Port Login Configuration with Authentication Mode Being Scheme.
	Specify to perform local authentication or remote authentication	
	Set user names and passwords locally or on AAA Server	

Note

To improve security and prevent attacks to the unused Sockets, TCP 23 and TCP 22, ports for Telnet and SSH services respectively, will be enabled or disabled after corresponding configurations.

- If the authentication mode is **none**, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is **password**, and the corresponding password has been set, TCP 23 will be enabled, and TCP 22 will be disabled.
- If the authentication mode is **scheme**, there are three scenarios: when the supported protocol is specified as **telnet**, TCP 23 will be enabled; when the supported protocol is specified as **ssh**, TCP 22 will be enabled; when the supported protocol is specified as **all**, both the TCP 23 and TCP 22 port will be enabled.

Telnet Configuration with Authentication Mode Being None

Configuration Procedure

Follow these steps to configure Telnet with the authentication mode being none:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	—
Configure not to authenticate users logging in to VTY user interfaces	**authentication-mode none**	Required By default, VTY users are authenticated after logging in.

Note that if you configure not to authenticate the users, the command level available to users logging in to a switch depends on the **user privilege level** *level* command

Configuration Example

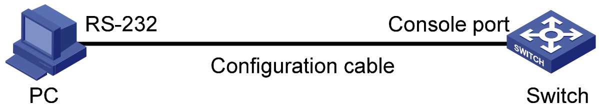
Network requirements

Assume current user logins through the console port, and the current user level is set to the administrator level (level 3). Perform the following configurations for users logging in through VTY 0 using Telnet.

- Do not authenticate the users.
- Commands of level 2 are available to the users.
- Telnet protocol is supported.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

Network diagram

Figure 3-1 Network diagram for Telnet configuration (with the authentication mode being none)



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Enter VTY 0 user interface view.

```
[Sysname] user-interface vty 0
```

Configure not to authenticate Telnet users logging in to VTY 0.

```
[Sysname-ui-vty0] authentication-mode none
```

Specify commands of level 2 are available to users logging in to VTY 0.

```
[Sysname-ui-vty0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[Sysname-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[Sysname-ui-vty0] idle-timeout 6
```

Telnet Configuration with Authentication Mode Being Password

Configuration Procedure

Follow these steps to configure Telnet with the authentication mode being password:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter one or more VTY user interface views	**user-interface vty** *first-number* [*last-number*]	—
Configure to authenticate users logging in to VTY user interfaces using the local password	**authentication-mode password**	Required
Set the local password	**set authentication password** { **cipher** | **simple** } *password*	Required

When the authentication mode is password, the command level available to users logging in to the user interface is determined by the **user privilege level** command.

Configuration Example

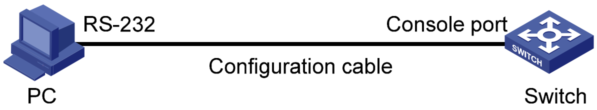
Network requirements

Assume current user logins through the console port and the current user level is set to the administrator level (level 3). Perform the following configurations for users logging in to VTY 0 using Telnet.

- Authenticate users using the local password.
- Set the local password to 123456 (in plain text).
- Commands of level 2 are available to the users.
- Telnet protocol is supported.
- The screen can contain up to 30 lines.
- The history command buffer can contain up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

Network diagram

Figure 3-2 Network diagram for Telnet configuration (with the authentication mode being password)



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Enter VTY 0 user interface view.

```
[Sysname] user-interface vty 0
```

Configure to authenticate users logging in to VTY 0 using the password.

```
[Sysname-ui-vty0] authentication-mode password
```

Set the local password to 123456 (in plain text).

```
[Sysname-ui-vty0] set authentication password simple 123456
```

Specify commands of level 2 are available to users logging in to VTY 0.

```
[Sysname-ui-vty0] user privilege level 2
```

Configure Telnet protocol is supported.

```
[Sysname-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[Sysname-ui-vty0] idle-timeout 6
```

Telnet Configuration with Authentication Mode Being Scheme

Configuration Procedure

Follow these steps to configure Telnet with the authentication mode being scheme:

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="2">Enter one or more VTY user interface views</td><td>user-interface vty first-number [last-number]</td><td>—</td></tr>
<tr><td colspan="2">Configure to authenticate users in the scheme mode</td><td>authentication-mode scheme [command-authorization]</td><td>Required
The specified AAA scheme determines what authentication mode is adopted, local or RADIUS.
Users are authenticated locally by default.</td></tr>
<tr><td colspan="2">Quit to system view</td><td>quit</td><td>—</td></tr>
<tr><td rowspan="3">Configure the authentication scheme</td><td>Enter the default ISP domain view</td><td>domain domain-name</td><td rowspan="3">Optional
By default, the local AAA scheme is applied. If you specify to apply the local AAA scheme, you need to perform the configuration concerning local user as well.
If you specify to apply RADIUS scheme, you need to perform the following configuration as well:
• Perform AAA&RADIUS configuration on the switch. (Refer to the AAA part for more.)
• Configure the user name and password accordingly on the AAA server. (Refer to the user manual of AAA server.)</td></tr>
<tr><td>Configure the AAA scheme to be applied to the domain</td><td>scheme { local | none | radius-scheme radius-scheme-name [local] }</td></tr>
<tr><td>Quit to system view</td><td>quit</td></tr>
<tr><td colspan="2">Create a local user and enter local user view</td><td>local-user user-name</td><td>No local user exists by default.</td></tr>
<tr><td colspan="2">Set the authentication password for the local user</td><td>password { simple | cipher } password</td><td>Required</td></tr>
<tr><td colspan="2">Specify the service type for VTY users</td><td>service-type telnet [level level]</td><td>Required</td></tr>
</table>

Note that:

If you configure to authenticate the users in the scheme mode, the command level available to the users logging in to the switch depends on the user level defined in the AAA scheme.

- When the AAA scheme is local, the user level depends on the **service-type** { **ftp** | **lan-access** | { **ssh** | **telnet** | **terminal** }* [**level** *level*] } command.
- When the AAA scheme is RADIUS, you need to specify the user level of a user on the corresponding RADIUS server.

Note

Refer to the *AAA* part of this manual for information about AAA, RADIUS.

Configuration Example

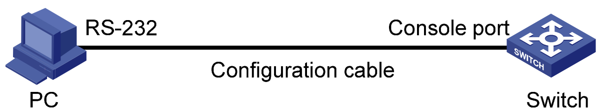
Network requirements

Assume current user logins through the console port and the user level is set to the administrator level (level 3). Perform the following configurations for users logging in to VTY 0 using Telnet.

- Configure the local user name as **guest**.
- Set the authentication password of the local user to **123456** (in plain text).
- Set the service type of VTY users to Telnet and the command level to 2.
- Configure to authenticate users logging in to VTY 0 in scheme mode.
- Only Telnet protocol is supported in VTY 0.
- The screen can contain up to 30 lines.
- The history command buffer can store up to 20 commands.
- The timeout time of VTY 0 is 6 minutes.

Network diagram

Figure 3-3 Network diagram for Telnet configuration (with the authentication mode being scheme)



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Create a local user named **guest** and enter local user view.

```
[Sysname] local-user guest
```

Set the authentication password of the local user to 123456 (in plain text).

```
[Sysname-luser-guest] password simple 123456
```

Set the service type to Telnet, Specify commands of level 2 are available to users logging in to VTY 0..

```
[Sysname-luser-guest] service-type telnet level 2
[Sysname-luser-guest] quit
```

Enter VTY 0 user interface view.

```
[Sysname] user-interface vty 0
```

Configure to authenticate users logging in to VTY 0 in the scheme mode.

```
[Sysname-ui-vty0] authentication-mode scheme
```

Configure Telnet protocol is supported.

```
[Sysname-ui-vty0] protocol inbound telnet
```

Set the maximum number of lines the screen can contain to 30.

```
[Sysname-ui-vty0] screen-length 30
```

Set the maximum number of commands the history command buffer can store to 20.

```
[Sysname-ui-vty0] history-command max-size 20
```

Set the timeout time to 6 minutes.

```
[Sysname-ui-vty0] idle-timeout 6
```

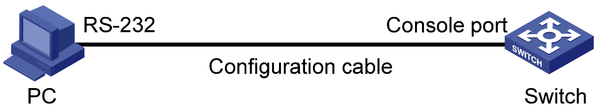
Telnetting to a Switch

Telnetting to a Switch from a Terminal

1) Assign an IP address to VLAN-interface 1 of the switch (VLAN 1 is the default VLAN of the switch).

- Connect the serial port of your PC/terminal to the console port of the switch, as shown in Figure 3-4

Figure 3-4 Diagram for establishing connection to a console port



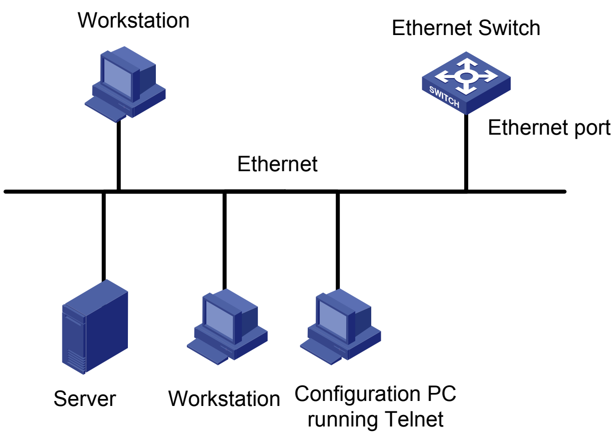
- Launch a terminal emulation utility (such as Terminal in Windows 3.X or HyperTerminal in Windows 95/Windows 98/Windows NT/Windows 2000/Windows XP) on the PC terminal, with the baud rate set to 19,200 bps, data bits set to 8, parity check set to none, and flow control set to none.
- Turn on the switch and press Enter as prompted. The prompt appears.
- Perform the following operations in the terminal window to assign IP address 202.38.160.92/24 to VLAN-interface 1 of the switch.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address 202.38.160.92 255.255.255.0
```

2) Perform Telnet-related configuration on the switch. Refer to Telnet Configuration with Authentication Mode Being None, Telnet Configuration with Authentication Mode Being Password, and Telnet Configuration with Authentication Mode Being Scheme for more.

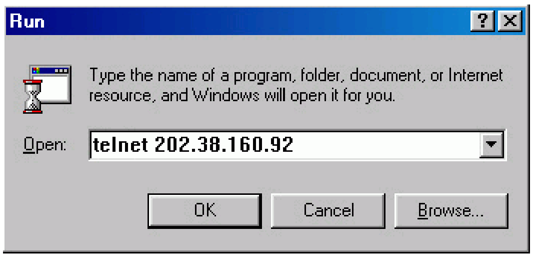
3) Connect your PC/terminal and the Switch to an Ethernet, as shown in Figure 3-5. Make sure the port through which the switch is connected to the Ethernet belongs to VLAN 1 and the route between your PC and VLAN-interface 1 is reachable.

Figure 3-5 Network diagram for Telnet connection establishment



4) Launch Telnet on your PC, with the IP address of VLAN-interface 1 of the switch as the parameter, as shown in Figure 3-6.

Figure 3-6 Launch Telnet



5) If the password authentication mode is specified, enter the password when the Telnet window displays “Login authentication” and prompts for login password. The CLI prompt (such as <Sysname>) appears if the password is correct. If all VTY user interfaces of the switch are in use, you will fail to establish the connection and receive the message that says “All user interfaces are used, please try later!”. A 3Com switch can accommodate up to five Telnet connections at same time.
6) After successfully Telnetting to the switch, you can configure the switch or display the information about the switch by executing corresponding commands. You can also type ? at any time for help. Refer to the relevant parts in this manual for the information about the commands.

Note

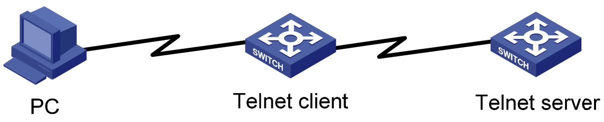
- A Telnet connection is terminated if you delete or modify the IP address of the VLAN interface in the Telnet session.
- By default, commands of level 0 are available to Telnet users authenticated by password. Refer to the CLI part for information about command hierarchy.

Telnetting to another Switch from the Current Switch

You can Telnet to another switch from the current switch. In this case, the current switch operates as the client, and the other operates as the server. If the interconnected Ethernet ports of the two switches are in the same LAN segment, make sure the IP addresses of the two management VLAN interfaces to which the two Ethernet ports belong to are of the same network segment, or the route between the two VLAN interfaces is available.

As shown in Figure 3-7, after Telnetting to a switch (labeled as Telnet client), you can Telnet to another switch (labeled as Telnet server) by executing the **telnet** command and then configure it.

Figure 3-7 Network diagram for Telnetting to another switch from the current switch



2) Perform Telnet-related configuration on the switch operating as the Telnet server. Refer to Telnet Configuration with Authentication Mode Being None, Telnet Configuration with Authentication Mode Being Password, and Telnet Configuration with Authentication Mode Being Scheme for more.
3) Telnet to the switch operating as the Telnet client.
4) Execute the following command on the switch operating as the Telnet client:

```
<Sysname> telnet xxxx
```

Note that xxxx is the IP address or the host name of the switch operating as the Telnet server. You can use the **ip host** to assign a host name to a switch.

1) After successful login, the CLI prompt (such as <Sysname>) appears. If all the VTY user interfaces of the switch are in use, you will fail to establish the connection and receive the message that says “All user interfaces are used, please try later!”.
2) After successfully Telnetting to the switch, you can configure the switch or display the information about the switch by executing corresponding commands. You can also type ? at any time for help. Refer to the following chapters for the information about the commands.

4 Logging In Using a Modem

Go to these sections for information you are interested in:

- Introduction
- Configuration on the Switch Side
- Modem Connection Establishment

Introduction

The administrator can log in to the console port of a remote switch using a modem through public switched telephone network (PSTN) if the remote switch is connected to the PSTN through a modem to configure and maintain the switch remotely. When a network operates improperly or is inaccessible, you can manage switches in the network remotely in this way.

To log in to a switch in this way, you need to configure the administrator side and the switch properly, as listed in the following table.

Table 4-1 Requirements for logging in to a switch using a modem

Item	Requirement
Administrator side	The PC can communicate with the modem connected to it.
	The modem is properly connected to PSTN.
	The telephone number of the switch side is available.
Switch side	The modem is connected to the console port of the switch properly.
	The modem is properly configured.
	The modem is properly connected to PSTN and a telephone set.
	The authentication mode and other related settings are configured on the switch. Refer to Table 2-3.

Configuration on the Switch Side

Modem Configuration

Perform the following configuration on the modem directly connected to the switch:

```
AT&F      ----------------------- Restore the factory settings
ATS0=1 ----------------------- Configure to answer automatically after the first ring
AT&D      ----------------------- Ignore DTR signal
AT&K0     ----------------------- Disable flow control
AT&R1     ----------------------- Ignore RTS signal
AT&S0     ----------------------- Set DSR to high level by force
ATEQ1&W   ----------------------- Disable the Modem from returning command response and the
result, save the changes
```

You can verify your configuration by executing the **AT&V** command.

Note

The configuration commands and the output of different modems may differ. Refer to the user manual of the modem when performing the above configuration.

Switch Configuration

Note

After logging in to a switch through its console port by using a modem, you will enter the AUX user interface. The corresponding configuration on the switch is the same as those when logging in to the switch locally through its console port except that:

- When you log in through the console port using a modem, the baud rate of the console port is usually set to a value lower than the transmission speed of the modem. Otherwise, packets may get lost.
- Other settings of the console port, such as the check mode, the stop bits, and the data bits, remain the default.

The configuration on the switch depends on the authentication mode the user is in. Refer to Table 2-3 for the information about authentication mode configuration.

Configuration on switch when the authentication mode is none

Refer to Console Port Login Configuration with Authentication Mode Being None.

Configuration on switch when the authentication mode is password

Refer to Console Port Login Configuration with Authentication Mode Being Password.

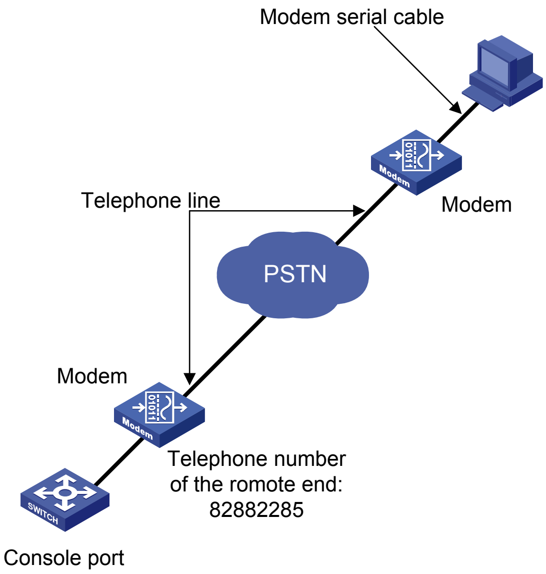
Configuration on switch when the authentication mode is scheme

Refer to Console Port Login Configuration with Authentication Mode Being Scheme.

Modem Connection Establishment

1) Before using Modem to log in the switch, perform corresponding configuration for different authentication modes on the switch. Refer to Console Port Login Configuration with Authentication Mode Being None, Console Port Login Configuration with Authentication Mode Being Password, and Console Port Login Configuration with Authentication Mode Being Scheme for more.
2) Perform the following configuration to the modem directly connected to the switch. Refer to Modem Configuration for related configuration.
3) Connect your PC, the modems, and the switch, as shown in Figure 4-1. Make sure the modems are properly connected to telephone lines.

Figure 4-1 Establish the connection by using modems



4) Launch a terminal emulation utility on the PC and set the telephone number to call the modem directly connected to the switch, as shown in Figure 4-2 through Figure 4-4. Note that you need to set the telephone number to that of the modem directly connected to the switch.

Figure 4-2 Create a connection

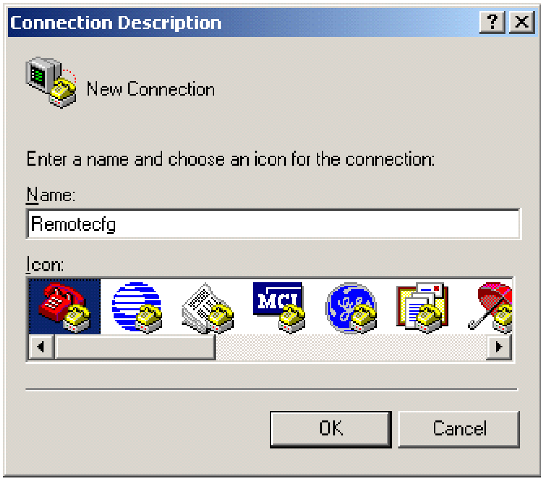


Figure 4-3 Set the telephone number

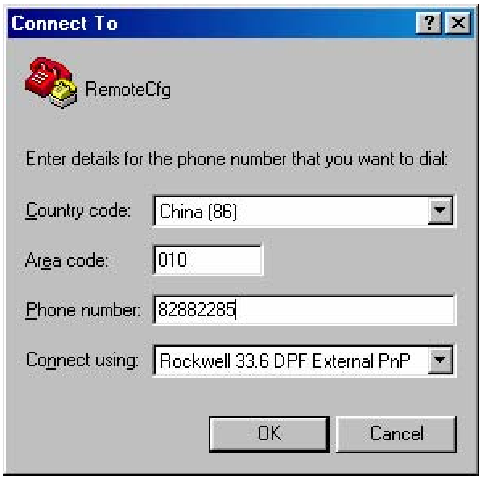
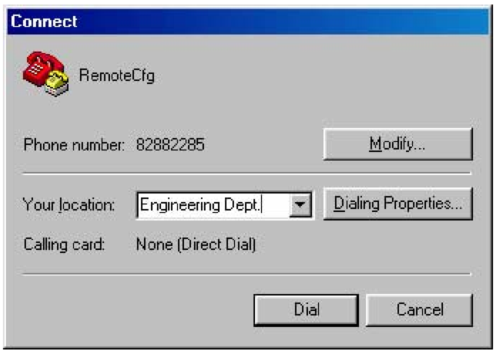


Figure 4-4 Call the modem



5) If the password authentication mode is specified, enter the password when prompted. If the password is correct, the prompt (such as <Sysname>) appears. You can then configure or manage the switch. You can also enter the character ? at anytime for help. Refer to the related parts in this manual for information about the configuration commands.

Note

If you perform no AUX user-related configuration on the switch, the commands of level 3 are available to modem users. Refer to the CLI part for information about command level.

---

5 CLI Configuration

When configuring CLI, go to these sections for information you are interested in:

- Introduction to the CLI
- Command Hierarchy
- CLI Views
- CLI Features

Introduction to the CLI

A command line interface (CLI) is a user interface to interact with a switch. Through the CLI on a switch, a user can enter commands to configure the switch and check output information to verify the configuration. Each 3com switch 4500 provides an easy-to-use CLI and a set of configuration commands for the convenience of the user to configure and manage the switch.

The CLI on the 3com switch 4500 provides the following features, and so has good manageability and operability.

- Hierarchical command protection: After users of different levels log in, they can only use commands at their own, or lower, levels. This prevents users from using unauthorized commands to configure switches.
- Online help: Users can gain online help at any time by entering a question mark (?).
- Debugging: Abundant and detailed debugging information is provided to help users diagnose and locate network problems.
- Command history function: This enables users to check the commands that they have lately executed and re-execute the commands.
- Partial matching of commands: The system will use partially matching method to search for commands. This allows users to execute a command by entering partially-spelled command keywords as long as the keywords entered can be uniquely identified by the system.

Command Hierarchy

Command Level and User Privilege Level

To restrict the different users' access to the device, the system manages the login users and all the commands by their privilege levels.

All the commands and login users are categorized into four levels, which are visit, monitor, system, and manage from low to high, and identified respectively by 0 through 3. After users at different privilege levels log in, they can only use commands at their own, or lower, levels. For example, level 2 users can only use level 0 through level 2 commands, not level 3 commands.

Command level

Based on user privilege, commands are classified into four levels, which default to:

- Visit level (level 0): Commands at this level are mainly used to diagnose network, and they cannot be saved in configuration file. For example, **ping**, **tracert** and **telnet** are level 0 commands.

- Monitor level (level 1): Commands at this level are mainly used to maintain the system and diagnose service faults, and they cannot be saved in configuration file. Such commands include **debugging** and **terminal**.
- System level (level 2): Commands at this level are mainly used to configure services. Commands concerning routing and network layers are at this level. These commands can be used to provide network services directly.
- Manage level (level 3): Commands at this level are associated with the basic operation modules and support modules of the system. These commands provide support for services. Commands concerning file system, FTP/TFTP/XModem downloading, user management, and level setting are at this level.

By using the **command-privilege level** command, the administrator can change the level of a command in a specific view as required. For details, refer to Modifying the Command Level.

User privilege level

Users logged into the switch fall into four user privilege levels, which correspond to the four command levels respectively. Users at a specific level can only use the commands at the same level or lower levels.

By default, the Console user (a user who logs into the switch through the Console port) is a level-3 user and can use commands of level 0 through level 3, while Telnet users are level-0 users and can only use commands of level 0.

You can use the **user privilege level** command to set the default user privilege level for users logging in through a certain user interface.

Note

If a user logs in using AAA authentication, the user privilege level depends on the configuration of the AAA scheme. For details, refer to *AAA Operation*.

Users can switch their user privilege level temporarily without logging out and disconnecting the current connection; after the switch, users can continue to configure the device without the need of relogin and reauthentication, but the commands that they can execute have changed. For details, refer to Switching User Level.

Modifying the Command Level

Modifying the command level

All the commands in a view are defaulted to different levels, as shown in Command level. The administrator can modify the command level based on users' needs to make users of a lower level use commands with a higher level or improve device security.

Follow these steps to set the level of a command in a specific view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the level of a command in a specific view	**command-privilege level** *level* **view** *view command*	Required

Caution

- You are recommended to use the default command level or modify the command level under the guidance of professional staff; otherwise, the change of command level may bring inconvenience to your maintenance and operation, or even potential security problem.
- When you change the level of a command with multiple keywords or arguments, you should input the keywords or arguments one by one in the order they appear in the command syntax. Otherwise, your configuration will not take effect. The values of the arguments should be within the specified ranges.
- After you change the level of a command in a certain view to be lower than the default level, change the level of the command used to enter the view accordingly.

Configuration example

The network administrator (a level 3 user) wants to change some TFTP commands (such as **tftp get**) from level 3 to level 0, so that general Telnet users (level 0 users) are able to download files through TFTP.

Change the **tftp get** command in user view (shell) from level 3 to level 0. (Originally, only level 3 users can change the level of a command.)

```
<Sysname> system-view
[Sysname] command-privilege level 0 view shell tftp
[Sysname] command-privilege level 0 view shell tftp 192.168.0.1
[Sysname] command-privilege level 0 view shell tftp 192.168.0.1 get
[Sysname] command-privilege level 0 view shell tftp 192.168.0.1 get bootrom.btm
```

After the above configuration, general Telnet users can use the **tftp get** command to download file bootrom.btm and other files from TFTP server 192.168.0.1 and other TFTP servers.

Switching User Level

Overview

Users can switch their user privilege level temporarily without logging out and disconnecting the current connection; after the switch, users can continue to configure the device without the need of relogin and reauthentication, but the commands that they can execute have changed.

For example, if the current user privilege level is 3, the user can configure system parameters; after switching the user privilege level to 0, the user can only execute some simple commands, like **ping** and **tracert**, and only a few **display** commands.

The switching of user privilege level is temporary, and effective for the current login; after the user relogs in, the user privilege restores to the original level.

To avoid misoperations, the administrators are recommended to log in to the device by using a lower privilege level and view device operating parameters, and when they have to maintain the device, they can switch to a higher level temporarily; when the administrators need to leave for a while or ask someone else to manage the device temporarily, they can switch to a lower privilege level before they leave to restrict the operation by others.

The high-to-low user level switching is unlimited. However, the low-to-high user level switching requires the corresponding authentication.

Complete the following tasks to configure user level switching:

Task		Remarks
The administrator configures the user level switching authentication policies	Adopting super password authentication for user level switching	Required
The user switches user level after logging in	Switching to a specific user level	Required

Adopting super password authentication for user level switching

With the super password set, you can pass the super password authentication successfully only when you provide the super password as prompted. If no super password is set, the system prompts "%Password is not set" when you attempt to switch to a higher user level. In this case, you cannot pass the super password authentication.

For example, after the administrator configures the **super password level** 3 **simple** 123 command, when users of level 0 through level 2 want to switch to user level 3, they need to input super password 123.

The following table lists the operations to configure super password authentication for user level switching, which can only be performed by level-3 users (administrators).

Follow these steps to set a password for use level switching:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the super password for user level switching	**super password** [**level** *level*] { **cipher** | **simple** } *password*	Required The configuration will take effect on all user interfaces. By default, the super password is not set.

Note

The super password is for level switching only and is different from the login password.

Switching to a specific user level

Follow these steps to switch to a specific user level:

To do…	Use the command…	Remarks
Switch to a specified user level	**super** [*level*]	Required Execute this command in user view.

Note

- If no user level is specified in the **super password** command or the **super** command, level 3 is used by default.
- For security purpose, the password entered is not displayed when you switch to another user level. You will remain at the original user level if you have tried three times but failed to enter the correct authentication information.

Configuration examples

After a general user telnets to the switch, his/her user level is 0. Now, the network administrator wants to allow general users to switch to level 3, so that they are able to configure the switch.

- The administrator configures the user level switching authentication policies.

Set the password used by the current user to switch to level 3.

```
[Sysname] super password level 3 simple 123
```

- A VTY 0 user switches its level to level 3 after logging in.

A VTY 0 user telnets to the switch, and then uses the set password to switch to user level 3.

```
<Sysname> super 3
 Password:
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

After configuring the switch, the general user switches back to user level 0.

```
<Sysname> super 0
User privilege level is 0, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

CLI Views

CLI views are designed for different configuration tasks. They are both correlated and distinguishing. For example, once a user logs into a switch successfully, the user enters user view, where the user can perform some simple operations such as checking the operation status and statistics information of the switch. After executing the **system-view** command, the user enters system view, where the user can go to other views by entering corresponding commands.

Table 5-1 lists the CLI views provided by the 3com switch 4500, operations that can be performed in different CLI views and the commands used to enter specific CLI views.

Table 5-1 CLI views

View	Available operation	Prompt example	Enter method	Quit method
User view	Display operation status and statistical information of the switch	<Sysname>	Enter user view once logging into the switch.	Execute the **quit** command to log out of the switch.
System view	Configure system parameters	[Sysname]	Execute the **system-view** command in user view.	Execute the **quit** or **return** command to return to user view.
Ethernet port view	Configure Ethernet port parameters	100 Mbps Ethernet port view: [Sysname-Ethernet1/0/1]	Execute the **interface ethernet** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
		1000 Mbps Ethernet port view: [Sysname-GigabitEthernet1/0/25]	Execute the **interface gigabitethernet** command in system view.	
Aux1/0/0 port (the console port) view	The 3com switch 4500 does not support configuration on port Aux1/0/0	[Sysname-Aux1/0/0]	Execute the **interface aux 1/0/0** command in system view	
VLAN view	Configure VLAN parameters	[Sysname-vlan1]	Execute the **vlan** command in system view.	
VLAN interface view	Configure VLAN interface parameters, including the management VLAN parameters	[Sysname-Vlan-interface1]	Execute the **interface Vlan-interface** command in system view.	
Loopback interface view	Configure loopback interface parameters	[Sysname-LoopBack0]	Execute the **interface loopback** command in system view.	
NULL interface view	Configure NULL interface parameters	[Sysname-NULL0]	Execute the **interface null** command in system view.	
Local user view	Configure local user parameters	[Sysname-luser-user1]	Execute the **local-user** command in system view.	
User interface view	Configure user interface parameters	[Sysname-ui-aux0]	Execute the **user-interface** command in system view.	

View	Available operation	Prompt example	Enter method	Quit method
FTP client view	Configure FTP client parameters	[ftp]	Execute the **ftp** command in user view.	
SFTP client view	Configure SFTP client parameters	sftp-client>	Execute the **sftp** command in system view.	
MST region view	Configure MST region parameters	[Sysname-mst-region]	Execute the **stp region-configuration** command in system view.	
Cluster view	Configure cluster parameters	[Sysname-cluster]	Execute the **cluster** command in system view.	
Public key view	Configure the RSA public key for SSH users	[Sysname-rsa-public-key]	Execute the **rsa peer-public-key** command in system view.	Execute the **peer-public-key end** command to return to system view.
	Configure the RSA or DSA public key for SSH users	[Sysname-peer-public-key]	Execute the **public-key peer** command in system view.	
Public key editing view	Edit the RSA public key for SSH users	[Sysname-rsa-key-code]	Execute the **public-key-code begin** command in public key view.	Execute the **public-key-code end** command to return to public key view.
	Edit the RSA or DSA public key for SSH users	[Sysname-peer-key-code]		
RIP view	Configure RIP protocol parameters	[Sysname-rip]	Execute the **rip** command in system view.	Execute the **quit** command to return to system view. Execute the **return** command to return to user view.
Routing policy view	Configure routing policy	[Sysname-route-policy]	Execute the **route-policy** command in system view.	
Basic ACL view	Define rules for a basic ACL (with ID ranging from 2000 to 2999)	[Sysname-acl-basic-2000]	Execute the **acl number** command in system view.	
Advanced ACL view	Define rules for an advanced ACL (with ID ranging from 3000 to 3999)	[Sysname-acl-adv-3000]	Execute the **acl number** command in system view.	
Layer 2 ACL view	Define rules for an layer 2 ACL (with ID ranging from 4000 to 4999)	[Sysname-acl-ethernetframe-4000]	Execute the **acl number** command in system view.	
User-defined ACL view	Define rules for a user-defined ACL (with ID ranging from 5000 to 5999)	[Sysname-acl-user-5000]	Execute the **acl number** command in system view.	

View	Available operation	Prompt example	Enter method	Quit method
RADIUS scheme view	Configure RADIUS scheme parameters	[Sysname-radius-1]	Execute the **radius scheme** command in system view.	
ISP domain view	Configure ISP domain parameters	[Sysname-isp-aaa123.net]	Execute the **domain** command in system view.	
Remote-ping test group view	Configure remote-ping test group parameters	[Sysname-remote-ping-a123-a123]	Execute the **remote-ping** command in system view.	
PoE profile view	Configure PoE profile parameters	[Sysname-poe-profile-a123]	Execute the **poe-profile** command in system view.	
Detected group view	Configure detected group parameters	[Sysname-detect-group-1]	Execute the **detect-group** command in system view.	
QinQ view	Configure QinQ parameters	[Sysname-Ethernet1/0/1-vid-20]	Execute the **vlan-vpn vid** command in Ethernet port view. The **vlan-vpn enable** command should be first executed.	Execute the **quit** command to return to Ethernet port view. Execute the **return** command to return to user view.

Note

The shortcut key <Ctrl+Z> is equivalent to the **return** command.

CLI Features

Online Help

When configuring the switch, you can use the online help to get related help information. The CLI provides two types of online help: complete and partial.

Complete online help

1) Enter a question mark (?) in any view on your terminal to display all the commands available in the view and their brief descriptions. The following takes user view as an example.

```
<Sysname> ?
User view commands:
  backup             Backup current configuration
  boot               Set boot option
```

```
  cd                Change current directory
  clock             Specify the system clock
  cluster           Run cluster command
  copy              Copy from one file to another
  debugging         Enable system debugging functions
  delete            Delete a file
  dir               List files on a file system
  display           Display current system information
```

<Other information is omitted>

2) Enter a command, a space, and a question mark (?).

If the question mark "?" is at a keyword position in the command, all available keywords at the position and their descriptions will be displayed on your terminal.

```
<Sysname> clock ?
  datetime     Specify the time and date
  summer-time  Configure summer time
  timezone     Configure time zone
```

If the question mark "?" is at an argument position in the command, the description of the argument will be displayed on your terminal.

```
[Sysname] interface vlan-interface ?
  <1-4094>  VLAN interface number
```

If only <cr> is displayed after you enter "?", it means no parameter is available at the "?" position, and you can enter and execute the command directly.

```
[Sysname] interface vlan-interface 1 ?
  <cr>
```

Partial online help

1) Enter a character/string, and then a question mark (?) next to it. All the commands beginning with the character/string will be displayed on your terminal. For example:

```
<Sysname> p?
   ping
   pwd
```

2) Enter a command, a space, a character/string and a question mark (?) next to it. All the keywords beginning with the character/string (if available) are displayed on your terminal. For example:

```
<Sysname> display v?
   version
   vlan
   voice
```

3) Enter the first several characters of a keyword of a command and then press <Tab>. If there is a unique keyword beginning with the characters just typed, the unique keyword is displayed in its complete form. If there are multiple keywords beginning with the characters, you can have them displayed one by one (in complete form) by pressing <Tab> repeatedly.

Terminal Display

The CLI provides the screen splitting feature to have display output suspended when the screen is full. When display output pauses, you can perform the following operations as needed (see Table 5-2).

Table 5-2 Display-related operations

Operation	Function
Press <Ctrl+C>	Stop the display output and execution of the command.
Press any character except <Space>, <Enter>, /, +, and - when the display output pauses	Stop the display output.
Press the space key	Get to the next page.
Press <Enter>	Get to the next line.

Command History

The CLI provides the command history function. You can use the **display history-command** command to view a specific number of latest executed commands and execute them again in a convenient way. By default, the CLI can store up to 10 latest executed commands for each user. You can view the command history by performing the operations listed in the following table:

Follow these steps to view history commands:

Purpose	Operation	Remarks
Display the latest executed history commands	Execute the **display history-command** command	This command displays the command history.
Recall the previous history command	Press the up arrow key or <Ctrl+P>	This operation recalls the previous history command (if available).
Recall the next history command	Press the down arrow key or <Ctrl+N>	This operation recalls the next history command (if available).

Note

- The Windows 9x HyperTerminal explains the up and down arrow keys in a different way, and therefore the two keys are invalid when you access history commands in such an environment. However, you can use <Ctrl+ P> and <Ctrl+ N> instead to achieve the same purpose.
- When you enter the same command multiple times consecutively, only one history command entry is created by the command line interface.

Error Prompts

If a command passes the syntax check, it will be successfully executed; otherwise, an error message will be displayed. Table 5-3 lists the common error messages.

Table 5-3 Common error messages

Error message	Remarks
Unrecognized command	The command does not exist.
	The keyword does not exist.
	The parameter type is wrong.
	The parameter value is out of range.
Incomplete command	The command entered is incomplete.
Too many parameters	The parameters entered are too many.
Ambiguous command	The parameters entered are ambiguous.
Wrong parameter	A parameter entered is wrong.
found at '^' position	An error is found at the '^' position.

Command Edit

The CLI provides basic command edit functions and supports multi-line editing. The maximum number of characters a command can contain is 254. Table 5-4 lists the CLI edit operations.

Table 5-4 Edit operations

Press…	To…
A common key	Insert the corresponding character at the cursor position and move the cursor one character to the right if the command is shorter than 254 characters.
Backspace key	Delete the character on the left of the cursor and move the cursor one character to the left.
Left arrow key or <Ctrl+B>	Move the cursor one character to the left.
Right arrow key or <Ctrl+F>	Move the cursor one character to the right.
Up arrow key or <Ctrl+P> Down arrow key or <Ctrl+N>	Display history commands.
<Tab>	Use the partial online help. That is, when you input an incomplete keyword and press <Tab>, if the input parameter uniquely identifies a complete keyword, the system substitutes the complete keyword for the input parameter; if more than one keywords match the input parameter, you can display them one by one (in complete form) by pressing <Tab> repeatedly; if no keyword matches the input parameter, the system displays your original input on a new line without any change.

6 Logging In Through the Web-based Network Management Interface

Go to these sections for information you are interested in:

- Introduction
- Establishing an HTTP Connection
- Configuring the Login Banner
- Enabling/Disabling the WEB Server

Introduction

Switch 4500 has a Web server built in. It enables you to log in to Switch 4500 through a Web browser and then manage and maintain the switch intuitively by interacting with the built-in Web server.

To log in to Switch 4500 through the built-in Web-based network management interface, you need to perform the related configuration on both the switch and the PC operating as the network management terminal.

Table 6-1 Requirements for logging in to a switch through the Web-based network management system

Item	Requirement
Switch	The VLAN interface of the switch is assigned an IP address, and the route between the switch and the Web network management terminal is reachable. (Refer to the *IP Address Configuration – IP Performance Configuration* and *Routing Protocol* parts for related information.)
	The user name and password for logging in to the Web-based network management system are configured.
PC operating as the network management terminal	IE is available.
	The IP address of the VLAN interface of the switch, the user name, and the password are available.

Establishing an HTTP Connection

1) Assign an IP address to VLAN-interface 1 of the switch (VLAN 1 is the default VLAN of the switch). See Telnetting to a Switch from a Terminal for related information.
2) Configure the user name and the password on the switch for the Web network management user to log in.

Create a Web user account, setting both the user name and the password to **admin** and the user level to 3.

```
<Sysname> system-view
[Sysname] local-user admin
[Sysname-luser-admin] service-type telnet level 3
[Sysname-luser-admin] password simple admin
```

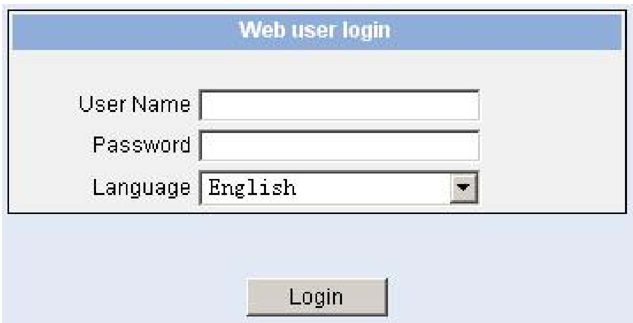
3) Establish an HTTP connection between your PC and the switch, as shown in Figure 6-1.

Figure 6-1 Establish an HTTP connection between your PC and the switch

4) Log in to the switch through IE. Launch IE on the Web-based network management terminal (your PC) and enter the IP address of the management VLAN interface of the switch in the address bar. (Make sure the route between the Web-based network management terminal and the switch is available.)

5) When the login authentication interface (as shown in Figure 6-2) appears, enter the user name and the password configured in step 2 and click <Login> to bring up the main page of the Web-based network management system.

Figure 6-2 The login page of the Web-based network management system



Configuring the Login Banner

Configuration Procedure

If a login banner is configured with the **header** command, when a user logs in through Web, the banner page is displayed before the user login authentication page. The contents of the banner page are the login banner information configured with the **header** command. Then, by clicking <Continue> on the banner page, the user can enter the user login authentication page, and enter the main page of the Web-based network management system after passing the authentication. If no login banner is configured by the **header** command, a user logging in through Web directly enters the user login authentication page.

Follow these steps to configure the login banner:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the banner to be displayed when a user logs in through Web	**header login** *text*	Required By default, no login banner is configured.

Configuration Example

Network requirements

- A user logs in to the switch through Web.
- The banner page is desired when a user logs into the switch.

Network diagram

Figure 6-3 Network diagram for login banner configuration

Configuration Procedure

Enter system view.

```
<Sysname> system-view
```

Configure the banner **Welcome** to be displayed when a user logs into the switch through Web.

```
[Sysname] header login %Welcome%
```

Assume that a route is available between the user terminal (the PC) and the switch. After the above-mentioned configuration, if you enter the IP address of the switch in the address bar of the browser running on the user terminal and press <Enter>, the browser will display the banner page, as shown in Figure 6-4.

Figure 6-4 Banner page displayed when a user logs in to the switch through Web

Click <Continue> to enter user login authentication page. You will enter the main page of the Web-based network management system if the authentication succeeds.

Enabling/Disabling the WEB Server

Follow these steps to enable/Disable the WEB Server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the Web server	**ip http shutdown**	Required By default, the Web server is enabled.
Disable the Web server	**undo ip http shutdown**	Required

Note

To improve security and prevent attack to the unused Sockets, TCP 80 port (which is for HTTP service) is enabled/disabled after the corresponding configuration.

- Enabling the Web server (by using the **undo ip http shutdown** command) opens TCP 80 port.
- Disabling the Web server (by using the **ip http shutdown** command) closes TCP 80 port.

7 Logging In Through NMS

Go to these sections for information you are interested in:

- Introduction
- Connection Establishment Using NMS

Introduction

You can also log in to a switch through a Network Management Station (NMS), and then configure and manage the switch through the agent software on the switch. Simple Network Management Protocol (SNMP) is applied between the NMS and the agent. Refer to the *SNMP-RMON* part for related information.

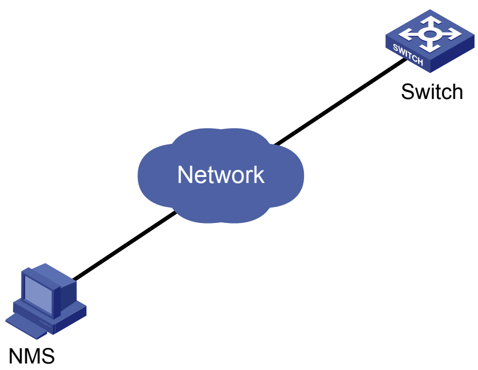
To log in to a switch through an NMS, you need to perform related configuration on both the NMS and the switch.

Table 7-1 Requirements for logging in to a switch through an NMS

Item	Requirement
Switch	The IP address of the VLAN interface of the switch is configured. The route between the NMS and the switch is reachable. (Refer to the *IP Address Configuration – IP Performance Configuration* and *Routing Protocol* parts for related information.)
	The basic SNMP functions are configured. (Refer to the *SNMP-RMON* part for related information.)
NMS	The NMS is properly configured. (Refer to the user manual of your NMS for related information.)

Connection Establishment Using NMS

Figure 7-1 Network diagram for logging in through an NMS



8 Configuring Source IP Address for Telnet Service Packets

Go to these sections for information you are interested in:

- Overview
- Configuring Source IP Address for Telnet Service Packets
- Displaying Source IP Address Configuration

Overview

You can configure source IP address or source interface for the Telnet server and Telnet client. This provides a way to manage services and enhances security.

The source IP address specified for Telnet service packets is the IP address of an Loopback interface or VLAN interface. After you specify the IP address of a virtual Loopback interface or an unused VLAN interface as the source IP address of Telnet service packets, the IP address is used as the source IP address no matter which interface of the switch is used to transmit packets between the Telnet client and the Telnet server. This conceals the IP address of the actual interface used. As a result, external attacks are guarded and the security is improved. On the other hand, you can configure the Telnet server to accept only Telnet service packets with specific source IP addresses to make sure specific users can log into the switch.

Configuring Source IP Address for Telnet Service Packets

This feature can be configured in either user view or system view. The configuration performed in user view takes effect for only the current session, while the configuration performed in system view takes effect for all the following sessions.

Configuration in user view

Table 8-1 Configure a source IP address for service packets in user view

Operation	Command	Description
Specify a source IP address for the Telnet client	**telnet** *remote-server* **source-ip** *ip-address*	Optional
Specify a source interface for the Telnet client	**telnet** *remote-server* **source-interface** *interface-type interface-number*	Optional

Configuration in system view

Table 8-2 Configure a source IP address for service packets in system view

Operation	Command	Description
Specify a source IP address for Telnet server	**telnet-server source-ip** *ip-address*	Optional

Operation	Command	Description
Specify a source interface for Telnet server	**telnet-server source-interface** *interface-type interface-number*	Optional
Specify source IP address for Telnet client	**telnet source-ip** *ip-address*	Optional
Specify a source interface for Telnet client	**telnet source-interface** *interface-type interface-number*	Optional

Note

To perform the configurations listed in Table 8-1 and Table 8-2, make sure that:

- The IP address specified is that of the local device.
- The interface specified exists.
- If a source IP address (or source interface) is specified, you need to make sure that the route between the IP addresses (or interface) of both sides is reachable.

Displaying Source IP Address Configuration

Execute the **display** command in any view to display the operation state after the above configurations. You can verify the configuration effect through the displayed information.

Table 8-3 Display the source IP address configuration

Operation	Command	Description
Display the source IP address configured for the Telnet client	**display telnet source-ip**	You can execute the two commands in any view.
Display the source IP address configured for the Telnet server	**display telnet-server source-ip**	

9 User Control

Go to these sections for information you are interested in:

- Introduction
- Controlling Telnet Users
- Controlling Network Management Users by Source IP Addresses
- Controlling Web Users by Source IP Address

Note

Refer to the *ACL* part for information about ACL.

Introduction

You can control users logging in through Telnet, SNMP and WEB by defining Access Control List (ACL), as listed in Table 9-1.

Table 9-1 Ways to control different types of login users

Login mode	Control method	Implementation	Related section
Telnet	By source IP address	Through basic ACL	Controlling Telnet Users
	By source and destination IP address	Through advanced ACL	
	By source MAC address	Through Layer 2 ACL	
SNMP	By source IP addresses	Through basic ACL	Controlling Network Management Users by Source IP Addresses
WEB	By source IP addresses	Through basic ACL	Controlling Web Users by Source IP Address
	Disconnect Web users by force	By executing commands in CLI	Logging Out a Web User

Controlling Telnet Users

Introduction

The controlling policy against Telnet users' access to VTY user interfaces is determined by referencing ACL. For the introduction to ACL, refer to the *ACL* part of this manual.

- If no ACL is configured on the VTY user interface, users are not controlled when establishing a Telnet connection using this user interface.
- If an ACL is configured on the VTY user interface, there will be two possibilities: if the packets for establishing a Telnet connection match the ACL rule configured on the VTY user interface, the connection will be permitted or denied according to the ACL rule; if not, the connection will be denied directly.

Controlling Telnet Users by ACL

Controlling Telnet users by ACL is achieved by the following two ways:

- **inbound**: Applies the ACL to the users Telnetting to the local switch through the VTY user interface.
- **outbound**: Applies the ACL to the users Telnetting to other devices through the current user interface. This keyword is unavailable to Layer 2 ACLs.

You can configure the following three types of ACLs as needed:

Table 9-2 ACL categories

Category	ACL number	Matching criteria
Basic ACL	2000 to 2999	Source IP address
Advanced ACL	3000 to 3999	Source IP address and destination IP address
Layer 2 ACL	4000 to 4999	Source MAC address

Note

Source and destination in this manual refer to a Telnet client and a Telnet server respectively.

- If the **inbound** keyword is specified, the Telnet client is the user telnetting to the local switch and the Telnet server is the local switch.
- If the **outbound** keyword is specified, the Telnet client is the local switch, and the Telnet server is another device to which the user is telnetting.

Follow these steps to control Telnet users by ACL:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **auto** | **config** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **deny | permit** } [*rule-string*]	Required
Quit to system view	**quit**	—
Enter user interface view	**user-interface** [*type*] *first-number* [*last-number*]	—

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td rowspan="2">Apply an ACL to control Telnet users by ACL</td><td>Apply a basic or advanced ACL to control Telnet users</td><td>acl acl-number { inbound | outbound }</td><td rowspan="2">Required
Use either command
• The inbound keyword specifies to filter the users trying to Telnet to the current switch.
• The outbound keyword specifies to filter users trying to Telnet to other switches from the current switch.</td></tr>
<tr><td>Apply a Layer 2 ACL to control Telnet users</td><td>acl acl-number inbound</td></tr>
</table>

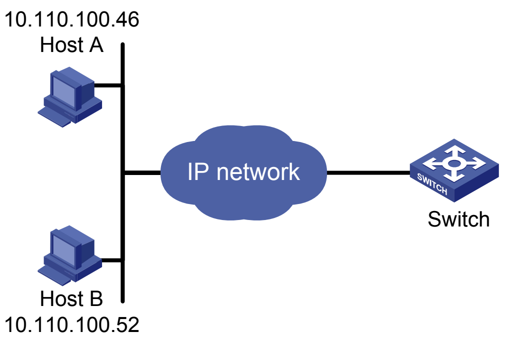
Configuration Example

Network requirements

Only the Telnet users sourced from the IP address of 10.110.100.52 are permitted to access the switch.

Network diagram

Figure 9-1 Network diagram for controlling Telnet users using ACLs



Configuration procedure

Define a basic ACL.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] quit
```

Apply the ACL.

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

Controlling Network Management Users by Source IP Addresses

You can manage Switch 4500 through network management software. Network management users can access switches through SNMP.

You need to perform the following two operations to control network management users by source IP addresses.

- Defining an ACL
- Applying the ACL to control users accessing the switch through SNMP

To control whether an NMS can manage the switch, you can use this function.

Prerequisites

The controlling policy against network management users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

Controlling Network Management Users by Source IP Addresses

Controlling network management users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Follow these steps to control network management users by source IP addresses:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **auto** | **config** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **deny** | **permit** } [*rule-string*]	Required
Quit to system view	**quit**	—
Apply the ACL while configuring the SNMP community name	**snmp-agent community** { **read** | **write** } *community-name* [**acl** *acl-number* | **mib-view** *view-name*]*	Required According to the SNMP version and configuration customs of NMS users, you can reference an ACL when configuring community name, group name or username. For the detailed configuration, refer to *SNMP-RMON* for more.
Apply the ACL while configuring the SNMP group name	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*] **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	
Apply the ACL while configuring the SNMP user name	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*] **snmp-agent usm-user v3** *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **des56** | **aes128** } *priv-password*]] [**acl** *acl-number*]	

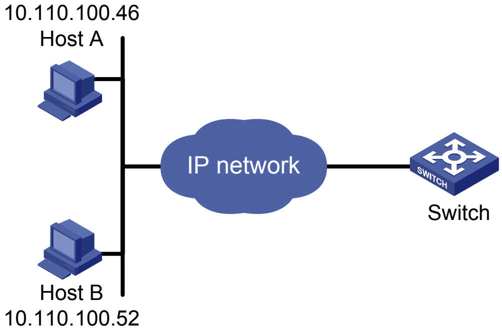
Configuration Example

Network requirements

Only SNMP users sourced from the IP addresses of 10.110.100.52 are permitted to log in to the switch.

Network diagram

Figure 9-2 Network diagram for controlling SNMP users using ACLs



Configuration procedure

Define a basic ACL.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] quit
```

Apply the ACL to only permit SNMP users sourced from the IP addresses of 10.110.100.52 to access the switch.

```
[Sysname] snmp-agent community read aaa acl 2000
[Sysname] snmp-agent group v2c groupa acl 2000
[Sysname] snmp-agent usm-user v2c usera groupa acl 2000
```

Controlling Web Users by Source IP Address

You can manage Switch 4500 remotely through Web. Web users can access a switch through HTTP connections.

You need to perform the following two operations to control Web users by source IP addresses.

- Defining an ACL
- Applying the ACL to control Web users

To control whether a Web user can manage the switch, you can use this function.

Prerequisites

The controlling policy against Web users is determined, including the source IP addresses to be controlled and the controlling actions (permitting or denying).

Controlling Web Users by Source IP Addresses

Controlling Web users by source IP addresses is achieved by applying basic ACLs, which are numbered from 2000 to 2999.

Follow these steps to control Web users by source IP addresses:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a basic ACL or enter basic ACL view	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	As for the **acl number** command, the **config** keyword is specified by default.
Define rules for the ACL	**rule** [*rule-id*] { **deny | permit** } [*rule-string*]	Required
Quit to system view	**quit**	—
Apply the ACL to control Web users	**ip http acl** *acl-number*	Optional By default, no ACL is applied for Web users.

Logging Out a Web User

The administrator can log out a Web user using the related command.

Follow the step below to log out a Web user:

To do…	Use the command…	Remarks
Log out a Web user	**free web-users** { **all** | **user-id** *user-id* | **user-name** *user-name* }	Required Available in user view

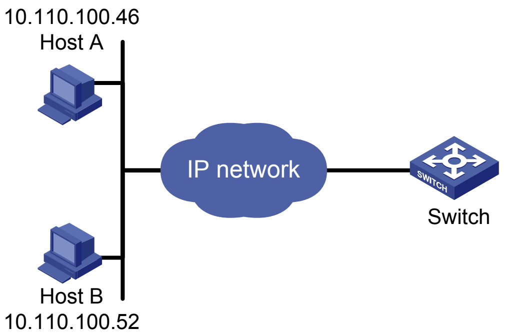
Configuration Example

Network requirements

Only the Web users sourced from the IP address of 10.110.100.52 are permitted to access the switch.

Network diagram

Figure 9-3 Network diagram for controlling Web users using ACLs



Configuration procedure

Define a basic ACL.

```
<Sysname> system-view
[Sysname] acl number 2030
[Sysname-acl-basic-2030] rule 1 permit source 10.110.100.52 0
```

```
[Sysname-acl-basic-2030] quit
```

Apply ACL 2030 to only permit the Web users sourced from the IP address of 10.110.100.52 to access the switch.

```
[Sysname] ip http acl 2030
```

Table of Contents

1 Configuration File Management

When configuring configuration file management, go to these sections for information you are interested in:

- Introduction to Configuration File
- Configuration Task List

Introduction to Configuration File

A configuration file records and stores user configurations performed to a switch. It also enables users to check switch configurations easily.

Types of configuration

The configuration of a switch falls into two types:

- Saved configuration, a configuration file used for initialization. If this file does not exist, the switch starts up without loading any configuration file.
- Current configuration, which refers to the user's configuration during the operation of a switch. This configuration is stored in Dynamic Random-Access Memory (DRAM). It is removed when rebooting.

Format of configuration file

Configuration files are saved as text files for ease of reading. They:

- Save configuration in the form of commands.
- Save only non-default configuration settings.
- The commands are grouped into sections by command view. The commands that are of the same command view are grouped into one section. Sections are separated by comment lines. (A line is a comment line if it starts with the character #.)
- The sections are listed in this order: system configuration section, logical interface configuration section, physical port configuration section, routing protocol configuration section, user interface configuration, and so on.
- End with a return.

The operating interface provided by the configuration file management function is user-friendly. With it, you can easily manage your configuration files.

Main/backup attribute of the configuration file

Main and backup indicate the main and backup attribute of the configuration file respectively. A main configuration file and a backup configuration file can coexist on the switch. As such, when the main configuration file is missing or damaged, the backup file can be used instead. This increases the safety and reliability of the file system compared with the switch that only support one configuration file. You can configure a file to have both main and backup attribute, but only one file of either main or backup attribute is allowed on a switch.

The following three situations are concerned with the main/backup attributes:

- When saving the current configuration, you can specify the file to be a main or backup or normal configuration file.
- When removing a configuration file from a switch, you can specify to remove the main or backup configuration file. Or, if it is a file having both main and backup attribute, you can specify to erase the main or backup attribute of the file.
- When setting the configuration file for next startup, you can specify to use the main or backup configuration file.

Startup with the configuration file

When booting, the system chooses the configuration files following the rules below:

1) If the main configuration file exists, the switch initializes with this configuration.
2) If the main configuration file does not exist but the backup configuration file exists, the switch initializes with the backup configuration.
3) If neither the main nor the backup configuration file exists, but the default configuration file **config.def** exists, the switch initializes with the default configuration file; if the default configuration file does not exist, the switch starts up without loading the configuration file.

Configuration Task List

Complete these tasks to configure configuration file management:

Task	Remarks
Saving the Current Configuration	Optional
Erasing the Startup Configuration File	Optional
Specifying a Configuration File for Next Startup	Optional

Saving the Current Configuration

You can modify the configuration on your switch at the command line interface (CLI). To use the modified configuration for your subsequent startups, you must save it (using the **save** command) as a configuration file.

Use the following command to save current configuration:

To do…	Use the command…	Remarks
Save current configuration	**save** [*cfgfile* | [**safely**] [**backup** | **main**]]	Required Available in any view

Modes in saving the configuration

- Fast saving mode. This is the mode when you use the **save** command without the **safely** keyword. The mode saves the file quicker but is likely to lose the original configuration file if the switch reboots or the power fails during the process.
- Safe mode. This is the mode when you use the **save** command with the **safely** keyword. The mode saves the file slower but can retain the original configuration file in the switch even if the switch reboots or the power fails during the process.

When you use the **save safely** command to save the configuration file, if the switch reboots or the power fails during the saving process, the switch initializes itself in the following two conditions when it starts up next time:

- If a configuration file with the extension **.cfg** exists in the Flash, the switch uses the configuration file to initialize itself when it starts up next time.
- If there is no **.cfg** configuration file in the Flash, but there is a configuration file with the extension **.cfgbak** (backup configuration file containing the original configuration information) or/and a configuration file with the extension **.cfgtmp** (temporary configuration file containing the current configuration information) in the Flash, you can change the extension **.cfgbak** or **.cfgtmp** to **.cfg** using the **rename** command. The switch will use the renamed configuration file to initialize itself when it starts up next time.

For details of the **rename** command, refer to the *File System Management* part of the manual.

Three attributes of the configuration file

- Main attribute. When you use the **save** [[**safely**] [**main**]] command to save the current configuration, the configuration file you get has main attribute. If this configuration file already exists and has backup attribute, the file will have both main and backup attributes after execution of this command. If the filename you entered is different from that existing in the system, this command will erase its main attribute to allow only one main attribute configuration file in the switch.
- Backup attribute. When you use the **save** [**safely**] **backup** command to save the current configuration, the configuration file you get has backup attribute. If this configuration file already exists and has main attribute, the file will have both main and backup attributes after execution of this command. If the filename you entered is different from that existing in the system, this command will erase its backup attribute to allow only one backup attribute configuration file in the switch.
- Normal attribute. When you use the **save** *cfgfile* command to save the current configuration, the configuration file you get has normal attribute if it is not an existing file. Otherwise, the attribute is dependent on the original attribute of the file.

Note

- It is recommended to adopt the fast saving mode in the conditions of stable power and adopt the safe mode in the conditions of unstable power or remote maintenance.
- If you use the **save** command after a fabric is formed on the switch, the units in the fabric save their own startup configuration files automatically.
- The extension name of the configuration file must be .cfg.

Erasing the Startup Configuration File

You can clear the configuration files saved on the switch through commands.

Use the following command to erase the configuration file:

To do…	Use the command…	Remarks
Erase the startup configuration file from the storage switch	**reset saved-configuration** [**backup** | **main**]	Required Available in user view

You may need to erase the configuration file for one of these reasons:

- After you upgrade software, the old configuration file does not match the new software.
- The startup configuration file is corrupted or not the one you needed.

The following two situations exist:

- While the **reset saved-configuration** [**main**] command erases the configuration file with main attribute, it only erases the main attribute of a configuration file having both main and backup attribute.
- While the **reset saved-configuration backup** command erases the configuration file with backup attribute, it only erases the backup attribute of a configuration file having both main and backup attribute.

Caution

This command will permanently delete the configuration file from the switch.

Specifying a Configuration File for Next Startup

Use the following command to specify a configuration file for next startup:

To do…	Use the command…	Remarks
Specify a configuration file for next startup	**startup saved-configuration** *cfgfile* [**backup** | **main**]	Required Available in user view

You can specify a configuration file to be used for the next startup and configure the main/backup attribute for the configuration file.

Assigning main attribute to the startup configuration file

- If you save the current configuration to the main configuration file, the system will automatically set the file as the main startup configuration file.
- You can also use the **startup saved-configuration** *cfgfile* [**main**] command to set the file as main startup configuration file.

Assigning backup attribute to the startup configuration file

- If you save the current configuration to the backup configuration file, the system will automatically set the file as the backup startup configuration file.
- You can also use the **startup saved-configuration** *cfgfile* **backup** command to set the file as backup startup configuration file.

Caution

The configuration file must use .cfg as its extension name and the startup configuration file must be saved at the root directory of the switch.

Displaying Switch Configuration

To do…	Use the command…	Remarks
Display the initial configuration file saved in the Flash of a switch	**display saved-configuration** [**unit** *unit-id*] [**by-linenum**]	Available in any view.
Display the configuration file used for this and next startup	**display startup** [**unit** *unit-id*]	
Display the current VLAN configuration of the switch	**display current-configuration vlan** [*vlan-id*] [**by-linenum**]	
Display the validated configuration in current view	**display this** [**by-linenum**]	
Display current configuration	**display current-configuration** [**configuration** [*configuration-type*] | **interface** [*interface-type*] [*interface-number*]] [**by-linenum**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	

Table of Contents

1 VLAN Overview

This chapter covers these topics:

- VLAN Overview
- Port-Based VLAN

VLAN Overview

Introduction to VLAN

The traditional Ethernet is a broadcast network, where all hosts are in the same broadcast domain and connected with each other through hubs or switches. Hubs and switches, which are the basic network connection devices, have limited forwarding functions.

- A hub is a physical layer device without the switching function, so it forwards the received packet to all ports except the inbound port of the packet.
- A switch is a link layer device which can forward a packet according to the MAC address of the packet. A switch builds a table of MAC addresses mapped to associated ports with that address and only sends a known MAC's traffic to one port. When the switch receives a broadcast packet or an unknown unicast packet whose MAC address is not included in the MAC address table of the switch, it will forward the packet to all the ports except the inbound port of the packet.

The above scenarios could result in the following network problems.

- Large quantity of broadcast packets or unknown unicast packets may exist in a network, wasting network resources.
- A host in the network receives a lot of packets whose destination is not the host itself, causing potential serious security problems.
- Related to the point above, someone on a network can monitor broadcast packets and unicast packets and learn of other activities on the network. Then they can attempt to access other resources on the network, whether or not they are authorized to do this.

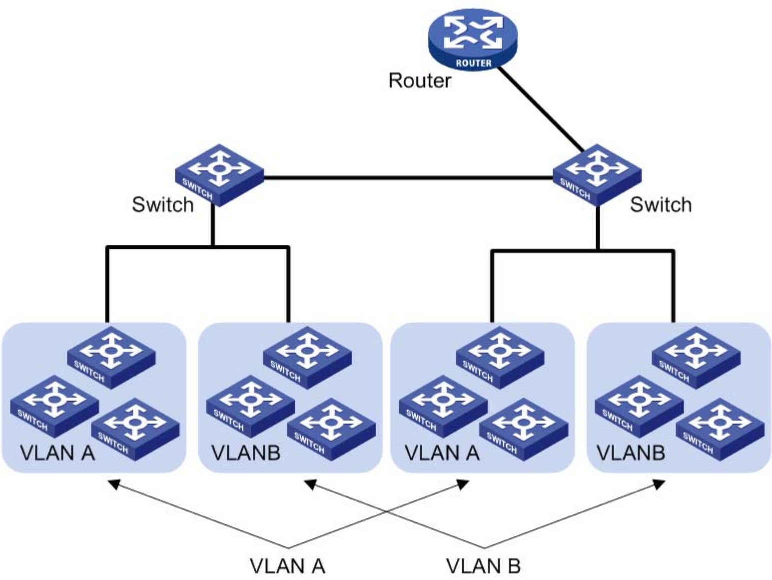
Isolating broadcast domains is the solution for the above problems. The traditional way is to use routers, which forward packets according to the destination IP address and does not forward broadcast packets in the link layer. However, routers are expensive and provide few ports, so they cannot split the network efficiently. Therefore, using routers to isolate broadcast domains has many limitations.

The Virtual Local Area Network (VLAN) technology is developed for switches to control broadcasts in LANs.

A VLAN can span across physical spaces. This enables hosts in a VLAN to be located in different physical locations.

By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate in the traditional Ethernet way. However, hosts in different VLANs cannot communicate with each other directly but need the help of network layer devices, such as routers and Layer 3 switches. Figure 1-1 illustrates a VLAN implementation.

Figure 1-1 A VLAN implementation



Advantages of VLANs

Compared with the traditional Ethernet, VLAN enjoys the following advantages.

- Broadcasts are confined to VLANs. This decreases bandwidth consumption and improves network performance.
- Network security is improved. Because each VLAN forms a broadcast domain, hosts in different VLANs cannot communicate with each other directly unless routers or Layer 3 switches are used.
- A more flexible way to establish virtual workgroups. VLAN can be used to create a virtual workgroup spanning physical network segments. When the physical position of a host changes within the range of the virtual workgroup, the host can access the network without changing its network configuration.

VLAN Principles

VLAN tag

To enable a network device to identify frames of different VLANs, a VLAN tag field is inserted into the data link layer encapsulation.

In 1999, IEEE issues the IEEE 802.1Q protocol to standardize VLAN implementation, defining the structure of VLAN-tagged packets.

In traditional Ethernet data frames, the type field of the upper layer protocol is encapsulated after the destination MAC address and source MAC address, as shown in Figure 1-2

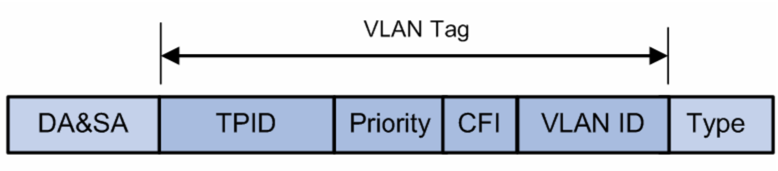
Figure 1-2 Encapsulation format of traditional Ethernet frames

DA&SA	Type	Data

In Figure 1-2 DA refers to the destination MAC address, SA refers to the source MAC address, and Type refers to the upper layer protocol type of the packet. IEEE 802.1Q protocol defines that a 4-byte VLAN

tag is encapsulated after the destination MAC address and source MAC address to show the information about VLAN.

Figure 1-3 Format of VLAN tag



As shown in Figure 1-3, a VLAN tag contains four fields, including the tag protocol identifier (TPID), priority, canonical format indicator (CFI), and VLAN ID.

- TPID is a 16-bit field, indicating that this data frame is VLAN-tagged. By default, it is 0x8100 in Ethernet switches.
- Priority is a 3-bit field, referring to 802.1p priority. Refer to the “QoS-QoS profile” part of this manual for details.
- CFI is a 1-bit field, indicating whether the MAC address is encapsulated in the standard format. 0 (the value of the CFI filed) indicates the MAC address is encapsulated in the standard format and 1 indicates the MAC address is not encapsulated in the standard format. The value is 0 by default.
- VLAN ID is a 12-bit field, indicating the ID of the VLAN to which this packet belongs. It is in the range of 0 to 4,095. Generally, 0 and 4,095 is not used, so the field is in the range of 1 to 4,094.

Note

The Ethernet II encapsulation format is used here. Besides the Ethernet II encapsulation format, other encapsulation formats such as 802.2 LLC and 802.2 SNAP are also supported by Ethernet. The VLAN tag fields are also added to frames encapsulated in these formats for VLAN identification.

VLAN ID identifies the VLAN to which a packet belongs. When a switch receives a packet carrying no VLAN tag, the switch encapsulates a VLAN tag with the default VLAN ID of the inbound port for the packet, and sends the packet to the default VLAN of the inbound port for transmission.

MAC address learning mechanism of VLANs

Switches make forwarding decisions based on destination MAC addresses. For this purpose, each switch maintains a MAC address table, of which each entry records the MAC address of a terminal connected to the switch and to which port this terminal is connected, assuming that no VLAN is involved. For the ease of management, a MAC learning mechanism is adopted on switches. With this mechanism, a switch can populate its MAC address table automatically by learning the source MAC address of incoming traffic and on which port the traffic is received. When forwarding traffic destined for the learned MAC address, the switch looks up the table and forwards the traffic according to the entry.

After VLANs are configured, a switch adopts one of the following MAC address learning mechanisms:

- Shared VLAN learning (SVL), where the switch records all learned MAC address entries in one MAC address table, regardless of in which VLAN they are learned. This table is called the shared MAC address forwarding table. Packets received in any VLAN on a port are forwarded according to this table.

- Independent VLAN learning (IVL), where the switch maintains an independent MAC address forwarding table for each VLAN. The source MAC address of a packet received in a VLAN on a port is recorded to the MAC address forwarding table of this VLAN only, and packets received in a VLAN are forwarded according to the MAC address forwarding table for the VLAN.

Currently, Switch 4500 series Ethernet switches adopt the IVL mode only. For more information about the MAC address forwarding table, refer to the "MAC Address Forwarding Table Management" part of the manual.

VLAN Interface

Hosts in different VLANs cannot communicate with each other directly unless routers or Layer 3 switches are used to do Layer 3 forwarding. The Switch 4500 series Ethernet switches support VLAN interfaces configuration to forward packets in Layer 3.

VLAN interface is a virtual interface in Layer 3 mode, used to realize the layer 3 communication between different VLANs, and does not exist on a switch as a physical entity. Each VLAN has a VLAN interface, which can forward packets of the local VLAN to the destination IP addresses at the network layer. Normally, since VLANs can isolate broadcast domains, each VLAN corresponds to an IP network segment. And a VLAN interface serves as the gateway of the segment to forward packets in Layer 3 based on IP addresses.

VLAN Classification

Depending on how VLANs are established, VLANs fall into the following six categories.

- Port-based VLANs
- MAC address-based VLANs
- Protocol-based VLANs
- IP-subnet-based VLANs
- Policy-based VLANs
- Other types

At present, the Switch 4500 series switches support the port-based VLANs.

Port-Based VLAN

Link Types of Ethernet Ports

You can configure the link type of a port as access, trunk, or hybrid. The three link types use different VLAN tag handling methods. When configuring the link type of a port, note that:

- An access port can belong to only one VLAN. Usually, ports directly connected to PCs are configured as access ports.
- A trunk port can carry multiple VLANs to receive and send traffic for them. Except traffic of the default VLAN, traffic passes through a trunk port will be VLAN tagged. Usually, ports connecting network devices are configured as trunk ports to allow members of the same VLAN to communicate with each other across multiple network devices.
- Like a trunk port, a hybrid port can carry multiple VLANs to receive and send traffic for them. Unlike a trunk port, a hybrid port allows traffic of all VLANs to pass through VLAN untagged. You can configure a port connected to a network device or user terminal as a hybrid port for access link connectivity or trunk connectivity.

Note

A hybrid port allows the packets of multiple VLANs to be sent untagged, but a trunk port only allows the packets of the default VLAN to be sent untagged.

The three types of ports can coexist on the same device.

Assigning an Ethernet Port to Specified VLANs

You can assign an Ethernet port to a VLAN to forward packets for the VLAN, thus allowing the VLAN on the current switch to communicate with the same VLAN on the peer switch.

An access port can be assigned to only one VLAN, while a hybrid or trunk port can be assigned to multiple VLANs.

Note

Before assigning an access or hybrid port to a VLAN, create the VLAN first.

Configuring the Default VLAN ID for a Port

An access port can belong to only one VLAN. Therefore, the VLAN an access port belongs to is also the default VLAN of the access port. A hybrid/trunk port can belong to multiple VLANs, so you should configure a default VLAN ID for the port.

After a port is added to a VLAN and configured with a default VLAN, the port receives and sends packets in a way related to its link type. For detailed description, refer to the following tables:

Table 1-1 Packet processing of an access port

Processing of an incoming packet		Processing of an outgoing packet
For an untagged packet	**For a tagged packet**	
Receive the packet and tag the packet with the default VLAN tag.	• If the VLAN ID is just the default VLAN ID, receive the packet. • If the VLAN ID is not the default VLAN ID, discard the packet.	Strip the tag from the packet and send the packet.

Table 1-2 Packet processing of a trunk port

Processing of an incoming packet		Processing of an outgoing packet
For an untagged packet	**For a tagged packet**	
• If the port has already been added to its default VLAN, tag the packet with the default VLAN tag and then forward the packet. • If the port has not been added to its default VLAN, discard the packet.	• If the VLAN ID is one of the VLAN IDs allowed to pass through the port, receive the packet. • If the VLAN ID is not one of the VLAN IDs allowed to pass through the port, discard the packet.	• If the VLAN ID is just the default VLAN ID, strip off the tag and send the packet. • If the VLAN ID is not the default VLAN ID, keep the original tag unchanged and send the packet.

Table 1-3 Packet processing of a hybrid port

Processing of an incoming packet		Processing of an outgoing packet
For an untagged packet	**For a tagged packet**	
• If the port has already been added to its default VLAN, tag the packet with the default VLAN tag and then forward the packet. • If the port has not been added to its default VLAN, discard the packet.	• If the VLAN ID is one of the VLAN IDs allowed to pass through the port, receive the packet. • If the VLAN ID is not one of the VLAN IDs allowed to pass through the port, discard the packet.	Send the packet if the VLAN ID is allowed to pass through the port. Use the **port hybrid vlan** command to configure whether the port keeps or strips off the tags when sending packets of a VLAN (including the default VLAN).

2 VLAN Configuration

When configuring VLAN, go to these sections for information you are interested in:

- VLAN Configuration
- Configuring a Port-Based VLAN

VLAN Configuration

VLAN Configuration Task List

Complete the following tasks to configure VLAN:

Task	Remarks
Basic VLAN Configuration	Required
Basic VLAN Interface Configuration	Optional
Displaying VLAN Configuration	Optional

Basic VLAN Configuration

Follow these steps to perform basic VLAN configuration:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create multiple VLANs in batch	**vlan** { *vlan-id1* **to** *vlan-id2* | **all** }	Optional
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	Required By default, there is only one VLAN, that is, the default VLAN (VLAN 1).
Assign a name for the current VLAN	**name** *text*	Optional By default, the name of a VLAN is its VLAN ID. **VLAN 0001** for example.
Specify the description string of the current VLAN	**description** *text*	Optional By default, the description string of a VLAN is its VLAN ID. **VLAN 0001** for example.

Caution

- VLAN 1 is the system default VLAN, which needs not to be created and cannot be removed, either.
- The VLAN you created in the way described above is a static VLAN. On the switch, there are dynamic VLANs which are registered through GVRP. For details, refer to "GVRP" part of this manual.
- When you use the **vlan** command to create VLANs, if the destination VLAN is an existing dynamic VLAN, it will be transformed into a static VLAN and the switch will output the prompt information.

Basic VLAN Interface Configuration

Configuration prerequisites

Before configuring a VLAN interface, create the corresponding VLAN.

Configuration procedure

Follow these steps to perform basic VLAN interface configuration:

<table>
<tr><th>To do...</th><th>Use the command...</th><th>Remarks</th></tr>
<tr><td>Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td>Create a VLAN interface and enter VLAN interface view</td><td>interface Vlan-interface vlan-id</td><td>Required
By default, there is no VLAN interface on a switch.</td></tr>
<tr><td>Specify the description string for the current VLAN interface</td><td>description text</td><td>Optional
By default, the description string of a VLAN interface is the name of this VLAN interface. Vlan-interface1 Interface for example.</td></tr>
<tr><td>Disable the VLAN interface</td><td>shutdown</td><td rowspan="2">Optional
By default, the VLAN interface is enabled. In this case, the VLAN interface's status is determined by the status of the ports in the VLAN, that is, if all ports of the VLAN are down, the VLAN interface is down (disabled); if one or more ports of the VLAN are up, the VLAN interface is up (enabled).
If you disable the VLAN interface, the VLAN interface will always be down, regardless of the status of the ports in the VLAN.</td></tr>
<tr><td>Enable the VLAN Interface</td><td>undo shutdown</td></tr>
</table>

Note

The operation of enabling/disabling a VLAN's VLAN interface does not influence the physical status of the Ethernet ports belonging to this VLAN.

Displaying VLAN Configuration

To do...	Use the command...	Remarks
Display the VLAN interface information	**display interface Vlan-interface** [*vlan-id*]	Available in any view.
Display the VLAN information	**display vlan** [*vlan-id* [**to** *vlan-id*] | **all** | **dynamic** | **static**]	

Configuring a Port-Based VLAN

Port-Based VLAN Configuration Task List

Complete these tasks to configure port-based VLAN:

Task	Remarks
Configuring the Link Type of an Ethernet Port	Optional
Assigning an Ethernet Port to a VLAN	Required
Configuring the Default VLAN for a Port	Optional
Displaying and Maintaining Port-Based VLAN	Optional

Configuring the Link Type of an Ethernet Port

Follow these steps to configure the link type of an Ethernet port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the port link type	**port link-type** { **access** | **hybrid** | **trunk** }	Required The link type of an Ethernet port is access by default.

Note

To change the link type of a port from trunk to hybrid or vice versa, you must set the link type to access first.

Assigning an Ethernet Port to a VLAN

You can assign an Ethernet port to a VLAN in Ethernet port view or VLAN view.

Caution

- You can assign an access port to a VLAN in either Ethernet port view or VLAN view.
- You can assign a trunk port or hybrid port to a VLAN only in Ethernet port view.

1) In Ethernet port view

Follow these steps to assign an Ethernet port to one or multiple VLANs:

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="2">Enter Ethernet port view</td><td>interface interface-type interface-number</td><td>—</td></tr>
<tr><td rowspan="3">Assign the current port to one or multiple VLANs</td><td>Access port</td><td>port access vlan vlan-id</td><td rowspan="3">Optional
By default, all Ethernet ports belong to VLAN 1.</td></tr>
<tr><td>Trunk port</td><td>port trunk permit vlan { vlan-id-list | all }</td></tr>
<tr><td>Hybrid port</td><td>port hybrid vlan vlan-id-list { tagged | untagged }</td></tr>
</table>

Note

When assigning an access or hybrid port to a VLAN, make sure the VLAN already exists.

2) In VLAN view

Follow these steps to assign one or multiple access ports to a VLAN in VLAN view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	Required If the specified VLAN does not exist, this command creates the VLAN first.
Assign the specified access port or ports to the current VLAN	**port** *interface-list*	Required By default, all ports belong to VLAN 1.

Configuring the Default VLAN for a Port

Because an access port can belong to only one VLAN, its default VLAN is the VLAN it resides in and cannot be configured.

This section describes how to configure a default VLAN for a trunk or hybrid port.

Follow these steps to configure the default VLAN for a port:

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="2">Enter Ethernet port view</td><td>interface interface-type interface-number</td><td>—</td></tr>
<tr><td rowspan="2">Configure the default VLAN for the current port</td><td>Trunk port</td><td>port trunk pvid vlan vlan-id</td><td rowspan="2">Optional
The link type of a port is access by default.</td></tr>
<tr><td>Hybrid port</td><td>port hybrid pvid vlan vlan-id</td></tr>
</table>

Caution

The local and remote trunk (or hybrid) ports must use the same default VLAN ID for the traffic of the default VLAN to be transmitted properly.

Displaying and Maintaining Port-Based VLAN

To do…	Use the command…	Remarks
Display the hybrid or trunk ports	**display port** { **hybrid** | **trunk** }	Available in any view.

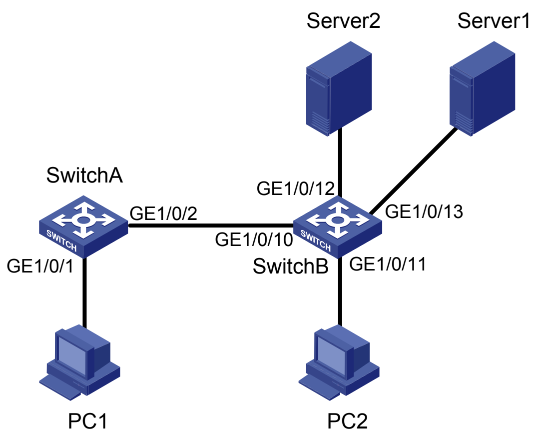
Port-Based VLAN Configuration Example

Network requirements

- As shown in Figure 2-1, Switch A and Switch B connect to PC 1/PC 2 and Server 1/Server 2 used by different departments.
- To isolate data between different departments, PC 1 and Server 1 are assigned to VLAN 100 with the descriptive string being Dept1; PC 2 and Server 2 are assigned to VLAN 200 with the descriptive string being Dept2.

Network diagram

Figure 2-1 Network diagram for VLAN configuration



Configuration procedure

- Configure Switch A.

Create VLAN 100, specify its descriptive string as **Dept1**, and add GigabitEthernet 1/0/1 to VLAN 100.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] description Dept1
[SwitchA-vlan100] port GigabitEthernet 1/0/1
[SwitchA-vlan100] quit
```

- Configure Switch B.

Create VLAN 100, specify its descriptive string as **Dept1**, and add GigabitEthernet 1/0/13 to VLAN 100.

```
<SwitchB> system-view
[SwitchB] vlan 100
[SwitchB-vlan100] description Dept1
[SwitchB-vlan100] port GigabitEthernet 1/0/13
[SwitchB-vlan103] quit
```

Create VLAN 200, specify its descriptive string as **Dept2** and add GigabitEthernet 1/0/11 and GigabitEthernet 1/0/12 to VLAN 200.

```
[SwitchB] vlan 200
[SwitchB-vlan200] description Dept2
[SwotchB-vlan200] port GigabitEthernet1/0/11 GigabitEthernet 1/0/12
[SwitchB-vlan200] quit
```

- Configure the link between Switch A and Switch B.

Because the link between Switch A and Switch B needs to transmit data of both VLAN 100 and VLAN 200, you can configure the ports at both ends of the link as trunk ports and permit packets of the two VLANs to pass through the two ports.

Configure GigabitEthernet 1/0/2 of Switch A.

```
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-type trunk
```

```
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 100
[SwitchA-GigabitEthernet1/0/2] port trunk permit vlan 200
```

Configure GigabitEthernet 1/0/10 of Switch B.

```
[SwitchB] interface GigabitEthernet 1/0/10
[SwitchB-GigabitEthernet1/0/10] port link-type trunk
[SwitchB-GigabitEthernet1/0/10] port trunk permit vlan 100
[SwitchB-GigabitEthernet1/0/10] port trunk permit vlan 200
```

Table of Contents

1 IP Addressing Configuration

Note

The term IP address used throughout this chapter refers to IPv4 address. For details about IPv6 address, refer to *IPv6 Management*.

When configuring IP addressing, go to these sections for information you are interested in:

- IP Addressing OverviewConfiguring IP Addresses
- Displaying IP Addressing Configuration
- IP Address Configuration Examples

IP Addressing Overview

IP Address Classes

On an IP network, a 32-bit address is used to identify a host. An example is 01010000100000001000000010000000 in binary. To make IP addresses in 32-bit form easier to read, they are written in dotted decimal notation, each being four octets in length, for example, 10.1.1.1 for the address just mentioned.

Each IP address breaks down into two parts:

- Net ID: The first several bits of the IP address defining a network, also known as class bits.
- Host ID: Identifies a host on a network.

IP addresses are divided into five classes, as shown in the following figure (in which the blue parts represent the address class).

Figure 1-1 IP address classes

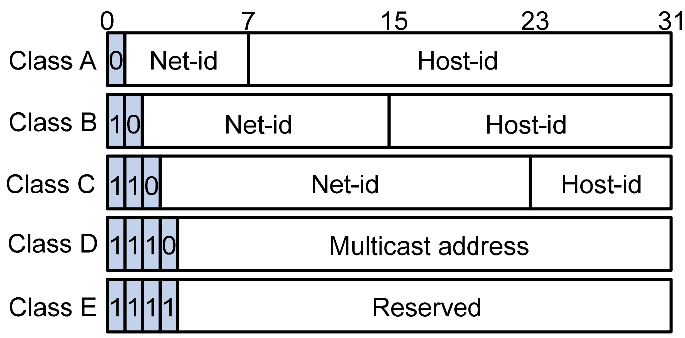


Table 1-1 describes the address ranges of these five classes.

Table 1-1 IP address classes and ranges

Class	Address range	Remarks
A	0.0.0.0 to 127.255.255.255	The IP address 0.0.0.0 is used by a host at bootstrap for temporary communication. This address is never a valid destination address. Addresses starting with 127 are reserved for loopback test. Packets destined to these addresses are processed locally as input packets rather than sent to the link.
B	128.0.0.0 to 191.255.255.255	—
C	192.0.0.0 to 223.255.255.255	—
D	224.0.0.0 to 239.255.255.255	Multicast addresses
E	240.0.0.0 to 255.255.255.255	Reserved for future use except for the broadcast address 255.255.255.255.

Special IP Addresses

The following IP addresses are for special use, and they cannot be used as host IP addresses:

- IP address with an all-zero net ID: Identifies a host on the local network. For example, IP address 0.0.0.16 indicates the host with a host ID of 16 on the local network.
- IP address with an all-zero host ID: Identifies a network.
- IP address with an all-one host ID: Identifies a directed broadcast address. For example, a packet with the destination address of 192.168.1.255 will be broadcasted to all the hosts on the network 192.168.1.0.

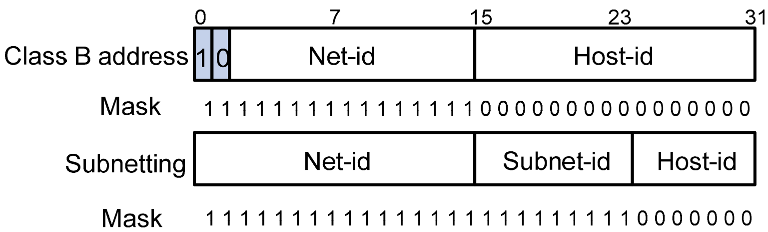
Subnetting and Masking

Subnetting was developed to address the risk of IP address exhaustion resulting from fast expansion of the Internet. The idea is to break a network down into smaller networks called subnets by using some bits of the host ID to create a subnet ID. To identify the boundary between the host ID and the combination of net ID and subnet ID, masking is used.

Each subnet mask comprises 32 bits related to the corresponding bits in an IP address. In a subnet mask, the part containing consecutive ones identifies the combination of net ID and subnet ID whereas the part containing consecutive zeros identifies the host ID.

Figure 1-2 shows how a Class B network is subnetted.

Figure 1-2 Subnet a Class B network



In the absence of subnetting, some special addresses such as the addresses with the net ID of all zeros and the addresses with the host ID of all ones, are not assignable to hosts. The same is true for

subnetting. When designing your network, you should note that subnetting is somewhat a tradeoff between subnets and accommodated hosts. For example, a Class B network can accommodate 65,534 (2^{16} – 2. Of the two deducted Class B addresses, one with an all-ones host ID is the broadcast address and the other with an all-zero host ID is the network address) hosts before being subnetted. After you break it down into 512 (2^9) subnets by using the first 9 bits of the host ID for the subnet, you have only 7 bits for the host ID and thus have only 126 (2^7 – 2) hosts in each subnet. The maximum number of hosts is thus 64,512 (512 × 126), 1022 less after the network is subnetted.

Class A, B, and C networks, before being subnetted, use these default masks (also called natural masks): 255.0.0.0, 255.255.0.0, and 255.255.255.0 respectively.

Configuring IP Addresses

Configuring IP Addresses

S4500 Series Ethernet Switches support assigning IP addresses to loopback interfaces and VLAN interfaces.

A loopback interface is a virtual interface. The physical layer state and link layer protocols of a loopback interface are always up unless the loopback interface is manually shut down. A loopback interface can be configured with an IP address, so routing protocols can be enabled on a loopback interface, and a loopback interface is capable of sending and receiving routing protocol packets.

Each VLAN needs an IP address so that it can be addressed. For more information about VLAN interfaces, refer to *VLAN Operation* in this manual.

Besides directly assigning an IP address to a VLAN interface, you may configure a VLAN interface to obtain an IP address through BOOTP or DHCP as alternatives. If you change the way an interface obtains an IP address, from manual assignment to BOOTP for example, the IP address obtained from BOOTP will overwrite the old one manually assigned.

Note

This chapter only covers how to assign an IP address manually. For the other two approaches, refer to the part discussing DHCP.

Follow these steps to configure an IP address for an interface:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Assign an IP address to the Interface	**ip address** *ip-address* { *mask* | *mask-length* }	Required No IP address is assigned by default.

Note

- A newly specified IP address overwrites the previous one if there is any.
- The IP address of a VLAN interface must not be on the same network segment as that of a loopback interface on a device.

Configuring Static Domain Name Resolution

Follow these steps to configure static domain name resolution:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a mapping between a host name and an IP address	**ip host** *hostname ip-address*	Required No IP address is assigned to a host name by default.

Note

- The IP address you assign to a host name last time will overwrite the previous one if there is any.
- You may create up to 50 static mappings between domain names and IP addresses.

Displaying IP Addressing Configuration

To do…	Use the command…	Remarks
Display static DNS database	**display ip host**	Available in any view
Display information about a specified or all Layer 3 interfaces	**display ip interface** [*interface-type interface-number*]	
Display brief configuration information about a specified or all Layer 3 interfaces	**display ip interface brief** [*interface-type* [*interface-number*]]	

IP Address Configuration Examples

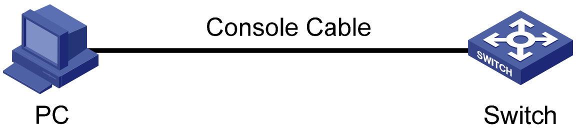
IP Address Configuration Example

Network requirement

Assign IP address 129.2.2.1 with mask 255.255.255.0 to VLAN-interface 1 of the switch.

Network diagram

Figure 1-3 Network diagram for IP address configuration



Configuration procedure

Configure an IP address for VLAN-interface 1.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 129.2.2.1 255.255.255.0
```

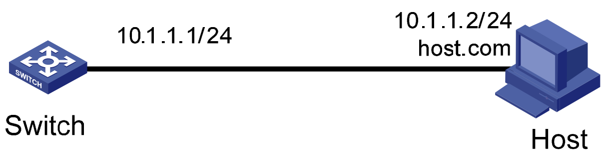
Static Domain Name Resolution Configuration Example

Network requirements

The switch uses static domain name resolution to access host 10.1.1.2 through domain name host.com.

Network diagram

Figure 1-4 Network diagram for static DNS configuration



Configuration procedure

Configure a mapping between host name host.com and IP address 10.1.1.2.

```
<Sysname> system-view
[Sysname] ip host host.com 10.1.1.2
```

Execute the **ping host.com** command to verify that the device can use static domain name resolution to get the IP address 10.1.1.2 corresponding to host.com.

```
[Sysname] ping host.com
  PING host.com (10.1.1.2): 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=127 time=3 ms
    Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=127 time=3 ms
    Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=127 time=2 ms
    Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=127 time=5 ms
    Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=127 time=3 ms


  --- host.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
```

```
round-trip min/avg/max = 2/3/5 ms
```

2 IP Performance Optimization Configuration

When optimizing IP performance, go to these sections for information you are interested in:

- IP Performance Overview
- Configuring IP Performance Optimization
- Displaying and Maintaining IP Performance Optimization Configuration

IP Performance Overview

Introduction to IP Performance Configuration

In some network environments, you can adjust the IP parameters to achieve best network performance. The IP performance optimization configuration supported by S4500 Series Ethernet Switches includes:

- Configuring TCP attributes
- Disabling ICMP to send error packets

Introduction to FIB

Every switch stores a forwarding information base (FIB). FIB is used to store the forwarding information of the switch and guide Layer 3 packet forwarding.

You can know the forwarding information of the switch by viewing the FIB table. Each FIB entry includes: destination address/mask length, next hop, current flag, timestamp, and outbound interface.

When the switch runs normally, its FIB table and routing table have the same contents.

Protocols and Standards

- RFC 793, *Transmission Control Protocol*
- RFC 1323, *TCP Extensions for High Performance*

Configuring IP Performance Optimization

IP Performance Optimization Configuration Task List

Complete the following tasks to configure IP performance Optimization:

Task	Remarks
Configuring TCP Attributes	Optional
Disabling Sending of ICMP Error Packets	Optional

Configuring TCP Attributes

TCP optional parameters that can be configured include:

- synwait timer: When sending a SYN packet, TCP starts the synwait timer. If no response packet is received within the synwait timer interval, the TCP connection cannot be created.
- finwait timer: When a TCP connection is changed into FIN_WAIT_2 state, the finwait timer is started. If no FIN packet is received within the timer timeout, the TCP connection will be terminated. If a FIN packet is received, the TCP connection state changes to TIME_WAIT. If a non-FIN packet is received, the system restarts the timer upon receiving the last non-FIN packet. The connection is broken after the timer expires.
- Size of TCP receive/send buffer

Follow these steps to configure TCP attributes:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the TCP synwait timer	**tcp timer syn-timeout** *time-value*	Optional 75 seconds by default.
Configure the TCP finwait timer	**tcp timer fin-timeout** *time-value*	Optional 675 seconds by default.
Configure the size of TCP receive/send buffer	**tcp window** *window-size*	Optional 8 kilobytes by default.

Disabling Sending of ICMP Error Packets

Sending error packets is a major function of the Internet Control Message Protocol (ICMP). In case of network abnormalities, ICMP packets are usually sent by the network or transport layer protocols to notify corresponding devices so as to facilitate management.

Advantages of sending ICMP error packets

ICMP redirect packets and destination unreachable packets are two kinds of ICMP error packets. Their sending conditions and functions are as follows.

1) Sending ICMP redirect packets

A host may have only a default route to the default gateway in its routing table after startup. The default gateway will send an ICMP redirect packet to the source host, telling it to reselect a better next hop to send the subsequent packets, if the following conditions are satisfied:

- The receiving and forwarding interfaces are the same.
- The selected route has not been created or modified by any ICMP redirect packet.
- The selected route is not the default route.
- There is no source route option in the data packet.

ICMP redirect packets simplify host administration and enables a host to gradually establish a sound routing table.

2) Sending ICMP destination unreachable packets

If a device receives an IP packet with an unreachable destination, it will drop the packet and send an ICMP destination unreachable error packet to the source.

Conditions for sending an ICMP unreachable packet:

- If neither a route nor the default route for forwarding a packet is available, the device will send a "network unreachable" ICMP error packet.

- If the destination of a packet is local while the transport layer protocol of the packet is not supported by the local device, the device sends a “protocol unreachable” ICMP error packet to the source.
- When receiving a packet with the destination being local and transport layer protocol being UDP, if the packet’s port number does not match the running process, the device will send the source a “port unreachable” ICMP error packet.
- If the source uses “strict source routing" to send packets, but the intermediate device finds that the next hop specified by the source is not directly connected, the device will send the source a “source routing failure” ICMP error packet.
- When forwarding a packet, if the MTU of the sending interface is smaller than the packet but the packet has “Don’t Fragment” set, the device will send the source a “fragmentation needed and Don’t Fragment (DF)-set” ICMP error packet.

Disadvantages of sending ICMP error packets

Although sending ICMP error packets facilitate control and management, it still has the following disadvantages:

- Sending a lot of ICMP packets will increase network traffic.
- If a device receives a lot of malicious packets that cause it to send ICMP error packets, its performance will be reduced.
- As the ICMP redirection function increases the routing table size of a host, the host’s performance will be reduced if its routing table becomes very large.
- If a host sends malicious ICMP destination unreachable packets, end users may be affected.

To prevent the above mentioned problems, you can disable the device from sending such ICMP error packets.

Follow these steps to disable sending ICMP error packets:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Disable sending of ICMP redirects	**undo icmp redirect send**	Required Enabled by default.
Disable sending of ICMP destination unreachable packets	**undo icmp unreach send**	Required Enabled by default.

Displaying and Maintaining IP Performance Optimization Configuration

To do…	Use the command…	Remarks
Display TCP connection status	**display tcp status**	Available in any view
Display TCP connection statistics	**display tcp statistics**	
Display UDP traffic statistics	**display udp statistics**	
Display IP traffic statistics	**display ip statistics**	

To do…	Use the command…	Remarks
Display ICMP traffic statistics	**display icmp statistics**	
Display the current socket information of the system	**display ip socket** [**socktype** *sock-type*] [*task-id socket-id*]	
Display the forwarding information base (FIB) entries	**display fib**	
Display the FIB entries matching the destination IP address	**display fib** *ip_address1* [{ *mask1* | *mask-length1* } [*ip_address2* { *mask2* | *mask-length2* } | **longer**] | **longer**]	
Display the FIB entries filtering through a specific ACL	**display fib acl** *number*	
Display the FIB entries in the buffer which begin with, include or exclude the specified character string.	**display fib** | { **begin** | **include** | **exclude** } *regular-expression*	
Display the FIB entries filtering through a specific prefix list	**display fib ip-prefix** *ip-prefix-name*	
Display the total number of the FIB entries	**display fib statistics**	
Clear IP traffic statistics	**reset ip statistics**	Available in user view
Clear TCP traffic statistics	**reset tcp statistics**	
Clear UDP traffic statistics	**reset udp statistics**	

Table of Contents

1 Voice VLAN Configuration

When configuring voice VLAN, go to these sections for information you are interested in:

- Voice VLAN Overview
- Voice VLAN Configuration
- Displaying and Maintaining Voice VLAN
- Voice VLAN Configuration Example

Voice VLAN Overview

Voice VLANs are allocated specially for voice traffic. After creating a voice VLAN and assigning ports that connect voice devices to the voice VLAN, you can have voice traffic transmitted in the dedicated voice VLAN and configure quality of service (QoS) parameters for the voice traffic to improve its transmission priority and ensure voice quality.

How an IP Phone Works

IP phones can convert analog voice signals into digital signals to enable them to be transmitted in IP-based networks. Used in conjunction with other voice devices, IP phones can offer large-capacity and low-cost voice communication solutions. As network devices, IP phones need IP addresses to operate properly in a network. An IP phone can acquire an IP address automatically or through manual configuration. The following part describes how an IP phone acquires an IP address automatically.

Note

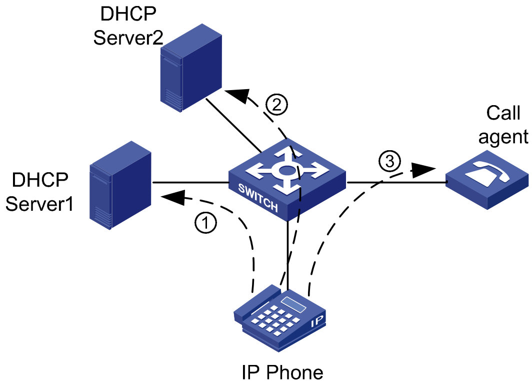
The following part only describes the common way for an IP phone to acquire an IP address. The detailed process may vary by manufacture. Refer to the corresponding user manual for the detailed information.

When an IP phone applies for an IP address from a DHCP server, the IP phone can also apply for the following extensive information from the DHCP server through the Option184 field:

- IP address of the network call processor (NCP)
- IP address of the secondary NCP server
- Voice VLAN configuration
- Failover call routing

Following describes the way an IP phone acquires an IP address.

Figure 1-1 Network diagram for IP phones



As shown in Figure 1-1, the IP phone needs to work in conjunction with the DHCP server and the NCP to establish a path for voice data transmission. An IP phone goes through the following three phases to become capable of transmitting voice data.

1) After the IP phone is powered on, it sends an untagged DHCP request message containing four special requests in the Option 184 field besides the request for an IP address. The message is broadcast in the default VLAN of the receiving port. After receiving the DHCP request message, DHCP Server 1, which resides in the default VLAN of the port receiving the message, responds as follows:

- If DHCP Server 1 does not support Option 184, it returns the IP address assigned to the IP phone but ignores the other four special requests in the Option 184 field. Without information about voice VLAN, the IP phone can only send untagged packets in the default VLAN of the port the IP phone is connected to. In this case, you need to manually configure the default VLAN of the port as a voice VLAN.

Note

In cases where an IP phone obtains an IP address from a DHCP server that does not support Option 184, the IP phone directly communicates through the gateway after it obtains an IP address. It does not go through the steps described below.

- If DHCP Server 1 supports Option 184, it returns the IP address assigned to the IP phone, the IP address of the NCP, the voice VLAN ID, and so on.

2) On acquiring the voice VLAN ID and NCP address from DHCP Server 1, the IP phone communicates with the specified NCP to download software, ignores the IP address assigned by DHCP Server 1, and sends a new DHCP request message carrying the voice VLAN tag to the voice VLAN.

3) After receiving the DHCP request, DHCP Server 2 residing in the voice VLAN assigns a new IP address to the IP phone and sends a tagged response message to the IP phone. After the IP phone receives the tagged response message, it sends voice data packets tagged with the voice VLAN tag to communicate with the voice gateway. In this case, the port connecting to the IP phone must be configured to allow the packets tagged with the voice VLAN tag to pass.

Note

- An untagged packet carries no VLAN tag.
- A tagged packet carries the tag of a VLAN.

To set an IP address and a voice VLAN for an IP phone manually, just make sure that the voice VLAN ID to be set is consistent with that of the switch and the NCP is reachable to the IP address to be set.

How Switch 4500 Series Switches Identify Voice Traffic

Switch 4500 series Ethernet switches determine whether a received packet is a voice packet by checking its source MAC address against an organizationally unique identifier (OUI) list. If a match is found, the packet is considered as a voice packet. Ports receiving packets of this type will be added to the voice VLAN automatically for transmitting voice data.

You can configure OUI addresses for voice packets or specify to use the default OUI addresses.

Note

An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address. Switch 4500 series Ethernet switches support OUI address mask configuration. You can adjust the matching depth of MAC address by setting different OUI address masks.

The following table lists the five default OUI addresses on Switch 4500 series switches.

Table 1-1 Default OUI addresses pre-defined on the switch

Number	OUI address	Vendor
1	0003-6b00-0000	Cisco phones
2	000f-e200-0000	H3C Aolynk phones
3	00d0-1e00-0000	Pingtel phones
4	00e0-7500-0000	Polycom phones
5	00e0-bb00-0000	3Com phones

Setting the Voice Traffic Transmission Priority

In order to improve transmission quality of voice traffic, the switch by default re-marks the priority of the traffic in the voice VLAN as follows:

- Set the CoS (802.1p) priority to 6.
- Set the DSCP value to 46.

Configuring Voice VLAN Assignment Mode of a Port

A port can work in automatic voice VLAN assignment mode or manual voice VLAN assignment mode. You can configure the voice VLAN assignment mode for a port according to data traffic passing through the port.

Processing mode of untagged packets sent by IP voice devices

- Automatic voice VLAN assignment mode. An Switch 4500 Ethernet switch automatically adds a port connecting an IP voice device to the voice VLAN by learning the source MAC address in the untagged packet sent by the IP voice device when it is powered on. The voice VLAN uses the aging mechanism to maintain the number of ports in the voice VLAN. When the aging timer expires, the ports whose OUI addresses are not updated (that is, no voice traffic passes) will be removed from the voice VLAN. In voice VLAN assignment automatic mode, ports can not be added to or removed from a voice VLAN manually.
- Manual voice VLAN assignment mode: In this mode, you need to add a port to a voice VLAN or remove a port from a voice VLAN manually.

Processing mode of tagged packets sent by IP voice devices

Tagged packets from IP voice devices are forwarded based on their tagged VLAN IDs, whether the automatic or manual voice VLAN assignment mode is used.

Caution

If the voice traffic transmitted by an IP voice device carries VLAN tags, and 802.1x authentication and guest VLAN is enabled on the port which the IP voice device is connected to, assign different VLAN IDs for the voice VLAN, the default VLAN of the port, and the 802.1x guest VLAN to ensure the effective operation of these functions.

Support for Voice VLAN on Various Ports

Voice VLAN packets can be forwarded by access ports, trunk ports, and hybrid ports. You can enable a trunk or hybrid port belonging to other VLANs to forward voice and service packets simultaneously by enabling the voice VLAN.

For different types of IP phones, the support for voice VLAN varies with port types and port configuration. For IP phones capable of acquiring IP address and voice VLAN automatically, the support for voice VLAN is described in Table 1-2.

Table 1-2 Matching relationship between port types and voice devices capable of acquiring IP address and voice VLAN automatically

Voice VLAN assignment mode	Voice traffic type	Port type	Supported or not
Automatic	Tagged voice traffic	Access	Not supported
		Trunk	Supported Make sure the default VLAN of the port exists and is not a voice VLAN, and the access port permits the traffic of the default VLAN.
		Hybrid	Supported Make sure the default VLAN of the port exists and is not a voice VLAN, and the default VLAN is in the list of the VLANs whose traffic is permitted by the access port.
	Untagged voice traffic	Access	Not supported, because the default VLAN of the port must be a voice VLAN and the access port is in the voice VLAN. This can be done by adding the port to the voice VLAN manually.
		Trunk	
		Hybrid	
Manual	Tagged voice traffic	Access	Not supported
		Trunk	Supported Make sure the default VLAN of the port exists and is not a voice VLAN, and the access port permits the traffic of the default VLAN and the voice VLAN.
		Hybrid	Supported Make sure the default VLAN of the port exists and is not a voice VLAN, the port permits the traffic of the default VLAN, and the voice VLAN is in the list of the tagged VLANs whose traffic is permitted by the access port.
	Untagged voice traffic	Access	Supported Make sure the default VLAN of the port is a voice VLAN.
		Trunk	Supported Make sure the default VLAN of the port is a voice VLAN and the port permits the traffic of the VLAN.
		Hybrid	Supported Make sure the default VLAN of the port is a voice VLAN and is in the list of untagged VLANs whose traffic is permitted by the port.

IP phones acquiring IP address and voice VLAN through manual configuration can forward only tagged traffic, so the matching relationship is relatively simple, as shown in Table 1-3:

Table 1-3 Matching relationship between port types and voice devices acquiring voice VLAN through manual configuration

Voice VLAN assignment mode	Port type	Supported or not
Automatic	Access	Not supported
	Trunk	Supported Make sure the default VLAN of the port exists and is not a voice VLAN, and the access port permits the traffic of the default VLAN.
	Hybrid	Supported Make sure the default VLAN of the port exists and is not a voice VLAN, and the default VLAN is in the list of the tagged VLANs whose traffic is permitted by the access port.
Manual	Access	Not supported
	Trunk	Supported Make sure the default VLAN of the port exists and is not a voice VLAN, and the access port permits the traffic of the default VLAN.
	Hybrid	Supported Make sure the default VLAN of the port exists and is not a voice VLAN, and the default VLAN and the voice VLAN is in the list of the tagged VLANs whose traffic is permitted by the access port.

Security Mode of Voice VLAN

The automatic mode and manual mode described earlier only apply to the process of assigning a port to the voice VLAN. After a port is assigned to the voice VLAN, the switch receives and forwards all voice VLAN-tagged traffic without matching the source MAC address of each received packet against its OUI list. For a port in the manual mode with the default VLAN as the voice VLAN, any untagged packet can be transmitted in the voice VLAN. This makes the voice VLAN vulnerable to flow attacks, because malicious users can create a large amount of voice VLAN-tagged packets to consume the voice VLAN bandwidth, affecting normal voice communication.

H3C series switches provide the security mode for voice VLAN to address this problem. When the voice VLAN works in security mode, the switch checks the source MAC address of each packet to enter the voice VLAN and drops the packets whose source MAC addresses do not match the OUI list. However, checking packets occupies lots of system resources. Therefore, in a relatively safe network, you can configure the voice VLAN to operate in normal mode.

The following table presents how a packet is handled when the voice VLAN is operating in security mode and normal mode.

Table 1-4 How a packet is handled when the voice VLAN is operating in different modes

Voice VLAN Mode	Packet Type	Processing Method
Security	Untagged packet	If the source MAC address of the packet

Voice VLAN Mode	Packet Type	Processing Method
	Packet carrying the voice VLAN tag	matches the OUI list, the packet is transmitted in the voice VLAN. Otherwise, the packet is dropped.
	Packet carrying any other VLAN tag	The packet is forwarded or dropped based on whether the receiving port is assigned to the carried VLAN. The processing method is irrelevant to the voice VLAN mode (security or normal).
Normal	Untagged packet	The source MAC address of the packet is not checked. All such packets can be transmitted in the voice VLAN.
	Packet carrying the voice VLAN tag	
	Packet carrying any other VLAN tag	The packet is forwarded or dropped based on whether the port is assigned to the carried VLAN. The processing method is irrelevant to the voice VLAN mode (security or normal).

Voice VLAN Configuration

Configuration Prerequisites

- Create the corresponding VLAN before configuring a voice VLAN.
- VLAN 1 (the default VLAN) cannot be configured as a voice VLAN.

Note

In case a connected voice device sends VLAN-tagged packets, ensure that the voice VLAN created on the switch is consistent with the VLAN corresponding to the VLAN tag carried in voice packets. Otherwise, the switch will not be able to properly receive voice packets.

Configuring the Voice VLAN to Operate in Automatic Voice VLAN Assignment Mode

Follow these steps to configure a voice VLAN to operate in automatic voice VLAN assignment mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set an OUI address that can be identified by the voice VLAN	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional By default, the switch determines the voice traffic according to the default OUI address.
Enable the voice VLAN security mode	**voice vlan security enable**	Optional By default, the voice VLAN security mode is enabled.

To do…	Use the command…	Remarks
Set the voice VLAN aging timer	**voice vlan aging** *minutes*	Optional The default aging timer is 1440 minutes.
Enable the voice VLAN function globally	**voice vlan** *vlan-id* **enable**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	Required
Enable the voice VLAN function on a port	**voice vlan enable**	Required By default, voice VLAN is disabled.
Enable the voice VLAN legacy function on the port	**voice vlan legacy**	Optional By default, voice VLAN legacy is disabled.
Set the voice VLAN assignment mode of the port to automatic	**voice vlan mode auto**	Optional The default voice VLAN assignment mode on a port is automatic.

Caution

For a port operating in automatic voice VLAN assignment mode, its default VLAN cannot be configured as the voice VLAN; otherwise the system prompts you for unsuccessful configuration.

Note

When the voice VLAN is working normally, if the device restarts or the Unit ID of a device in a XRN fabric changes, in order to make the established voice connections work normally, the system does not need to be triggered by the voice traffic to add the port in automatic voice VLAN assignment mode to the local devices as well as the XRN of the voice VLAN but does so immediately after the restart or the changes.

Configuring the Voice VLAN to Operate in Manual Voice VLAN Assignment Mode

Follow these steps to configure a voice VLAN to operate in manual voice VLAN assignment mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set an OUI address that can be identified by the voice VLAN	**voice vlan mac-address** *oui* **mask** *oui-mask* [**description** *text*]	Optional Without this address, the default OUI address is used.

<table>
<tr><th colspan="3">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="3">Enable the voice VLAN security mode</td><td>voice vlan security enable</td><td>Optional
By default, the voice VLAN security mode is enabled.</td></tr>
<tr><td colspan="3">Set the voice VLAN aging timer</td><td>voice vlan aging minutes</td><td>Optional
The default aging timer is 1,440 minutes.</td></tr>
<tr><td colspan="3">Enable the voice VLAN function globally</td><td>voice vlan vlan-id enable</td><td>Required</td></tr>
<tr><td colspan="3">Enter port view</td><td>interface interface-type interface-number</td><td>Required</td></tr>
<tr><td colspan="3">Enable voice VLAN on a port</td><td>voice vlan enable</td><td>Required
By default, voice VLAN is disabled on a port.</td></tr>
<tr><td colspan="3">Enable the voice VLAN legacy function on the port</td><td>voice vlan legacy</td><td>Optional
By default, voice VLAN legacy is disabled.</td></tr>
<tr><td colspan="3">Set voice VLAN assignment mode on a port to manual</td><td>undo voice vlan mode auto</td><td>Required
The default voice VLAN assignment mode on a port is automatic.</td></tr>
<tr><td colspan="3">Quit to system view</td><td>quit</td><td>—</td></tr>
<tr><td rowspan="5">Add a port in manual voice VLAN assignment mode to the voice VLAN</td><td rowspan="2">Access port</td><td>Enter VLAN view</td><td>vlan vlan-id</td><td rowspan="4">Required
By default, all the ports belong to VLAN 1.</td></tr>
<tr><td>Add the port to the VLAN</td><td>port interface-list</td></tr>
<tr><td rowspan="3">Trunk or Hybrid port</td><td>Enter port view</td><td>interface interface-type interface-num</td></tr>
<tr><td>Add the port to the VLAN</td><td>port trunk permit vlan vlan-id
port hybrid vlan vlan-id { tagged | untagged }</td></tr>
<tr><td>Configure the voice VLAN to be the default VLAN of the port</td><td>port trunk pvid vlan vlan-id
port hybrid pvid vlan vlan-id</td><td>Optional
Refer to Table 1-2 to determine whether or not this operation is needed.</td></tr>
</table>

Caution

- The voice VLAN function can be enabled for only one VLAN at one time.
- If the Link Aggregation Control Protocol (LACP) is enabled on a port, voice VLAN feature cannot be enabled on it.
- Voice VLAN function can be enabled only for the static VLAN. A dynamic VLAN cannot be configured as a voice VLAN.
- When ACL number applied to a port reaches to its threshold, voice VLAN cannot be enabled on this port. You can use the **display voice vlan error-info** command to locate such ports.
- When a voice VLAN operates in security mode, the device in it permits only the packets whose source addresses are the identified voice OUI addresses. Packets whose source addresses cannot be identified, including certain authentication packets (such as 802.1x authentication packets), will be dropped. Therefore, you are suggested not to transmit both voice data and service data in a voice VLAN. If you have to do so, make sure that the voice VLAN does not operate in security mode.
- The voice VLAN legacy feature realizes the communication between 3Com device and other vendor's voice device by automatically adding the voice VLAN tag to the voice data coming from other vendors' voice device. The **voice vlan legacy** command can be executed before voice VLAN is enabled globally and on a port, but it takes effect only after voice VLAN is enabled globally and on the port.

Note

To assign a trunk port or a hybrid port to the voice VLAN, refer to *VLAN Configuration* of this manual for the related command.

Displaying and Maintaining Voice VLAN

To do…	Use the command…	Remarks
Display information about the ports on which voice VLAN configuration fails	**display voice vlan error-info**	In any view
Display the voice VLAN configuration status	**display voice vlan status**	
Display the OUI list	**display voice vlan oui**	
Display the ports operating in the voice VLAN	**display vlan** *vlan-id*	

Voice VLAN Configuration Example

Voice VLAN Configuration Example (Automatic Voice VLAN Assignment Mode)

Network requirements

As shown in Figure 1-2,

The MAC address of IP phone A is 0011-1100-0001. The phone connects to a downstream device named PC A whose MAC address is 0022-1100-0002 and to GigabitEthernet 1/0/1 on an upstream device named Device A.

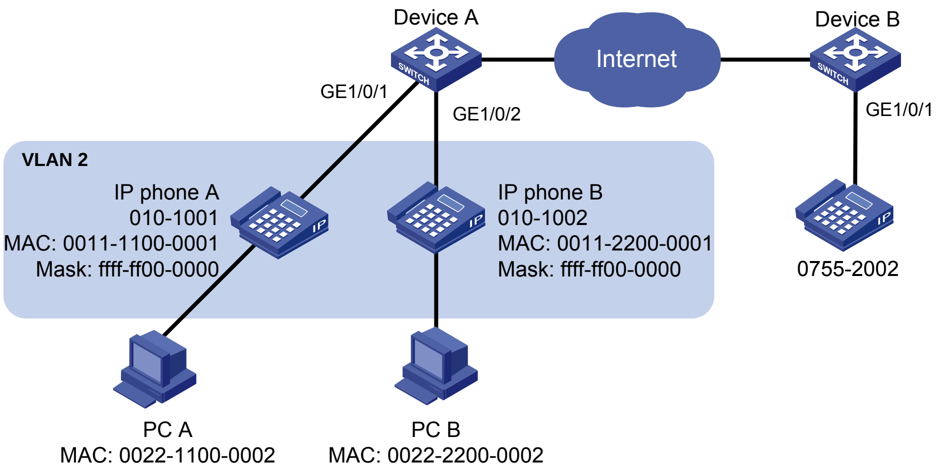
The MAC address of IP phone B is 0011-2200-0001. The phone connects to a downstream device named PC B whose MAC address is 0022-2200-0002 and to Ethernet GigabitEthernet1/0/2 on Device A.

Device A uses voice VLAN 2 to transmit voice packets for IP phone A and IP phone B.

Configure GigabitEthernet 1/0/1 and GigabitEthernet 1/0/2 to work in automatic voice VLAN assignment mode. In addition, if one of them has not received any voice packet in 30 minutes, the port is removed from the corresponding voice VLAN automatically.

Network diagram

Figure 1-2 Network diagram for voice VLAN configuration (automatic mode)



Configuration procedure

Create VLAN 2.

```
<DeviceA> system-view
[DeviceA] vlan 2
```

Set the voice VLAN aging time to 30 minutes.

```
[DeviceA] voice vlan aging 30
```

Configure VLAN 2 as a voice VLAN.

```
[DeviceA] voice vlan 2 enable
```

Since GigabitEthernet 1/0/1 may receive both voice traffic and data traffic at the same time, to ensure the quality of voice packets and effective bandwidth use, configure voice VLANs to work in security mode, that is, configure the voice VLANs to transmit only voice packets. (Optional. By default, voice VLANs work in security mode.)

```
[DeviceA] voice vlan security enable
```

Configure the allowed OUI addresses as MAC addresses prefixed by 0011-1100-0000 or 0011-2200-0000. In this way, Device A identifies packets whose MAC addresses match any of the configured OUI addresses as voice packets.

```
[DeviceA] voice vlan mac-address 0011-1100-0001 mask ffff-ff00-0000 description IP phone A
[DeviceA] voice vlan mac-address 0011-2200-0001 mask ffff-ff00-0000 description IP phone B
```

Configure GigabitEthernet 1/0/1 to operate in automatic voice VLAN assignment mode. (Optional. By default, a port operates in automatic voice VLAN assignment mode.)

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] voice vlan mode auto
```

Configure GigabitEthernet 1/0/1 as a hybrid port.

```
[DeviceA-GigabitEthernet1/0/1] port link-type hybrid
```

Configure VLAN 2 as the voice VLAN for GigabitEthernet 1/0/1.

```
[DeviceA-GigabitEthernet1/0/1] voice vlan enable
[DeviceA-GigabitEthernet1/0/1] quit
```

Configure GigabitEthernet 1/0/2.

```
[DeviceA] interface gigabitethernet 1/0/2
[DeviceA-GigabitEthernet1/0/2] voice vlan mode auto
[DeviceA-GigabitEthernet1/0/2] port link-type access
 Please wait... Done.
[DeviceA-GigabitEthernet1/0/2] port link-type hybrid
[DeviceA-GigabitEthernet1/0/2] voice vlan enable
```

Verification

Display the OUI addresses, OUI address masks, and description strings supported currently.

```
<DeviceA> display voice vlan oui
Oui Address     Mask            Description
0003-6b00-0000  ffff-ff00-0000  Cisco phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0011-1100-0000  ffff-ff00-0000  IP phone A
0011-2200-0000  ffff-ff00-0000  IP phone B
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Display the current states of voice VLANs.

```
<DeviceA> display voice vlan state
Voice Vlan status: ENABLE
Voice Vlan ID: 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440 minutes
Current voice vlan enabled port mode:
PORT                           MODE
----------------------------------------
GigabitEthernet1/0/1           AUTO
GigabitEthernet1/0/2           AUTO
```

Voice VLAN Configuration Example (Manual Voice VLAN Assignment Mode)

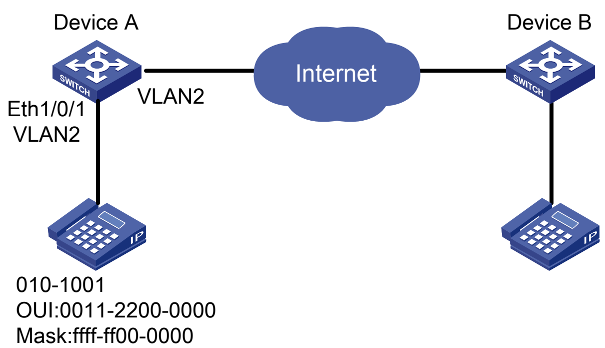
Network requirements

Create a voice VLAN and configure it to operate in manual voice VLAN assignment mode. Add the port to which an IP phone is connected to the voice VLAN to enable voice traffic to be transmitted within the voice VLAN.

- Create VLAN 2 and configure it as a voice VLAN. Set the voice VLAN to operate in security mode
- The IP phone sends untagged packets. It is connected to Ethernet 1/0/1, a hybrid port. Set this port to operate in manual voice VLAN assignment mode.
- You need to add a user-defined OUI address 0011-2200-000, with the mask being ffff-ff00-0000 and the description string being “test”.

Network diagram

Figure 1-3 Network diagram for voice VLAN configuration (manual voice VLAN assignment mode)



Configuration procedure

Enable the security mode for the voice VLAN so that the ports in the voice VLAN permit valid voice packets only. This operation is optional. The security mode is enabled by default.

```
<DeviceA> system-view
[DeviceA] voice vlan security enable
```

Add a user-defined OUI address 0011-2200-000 and set the description string to “test”.

```
[DeviceA] voice vlan mac-address 0011-2200-0000 mask ffff-ff00-0000 description test
```

Create VLAN 2 and configure it as a voice VLAN.

```
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] voice vlan 2 enable
```

Configure Ethernet 1/0/1 to operate in manual voice VLAN assignment mode.

```
[DeviceA] interface Ethernet 1/0/1
[DeviceA-Ethernet1/0/1] undo voice vlan mode auto
```

Configure Ethernet 1/0/1 as a hybrid port.

```
[DeviceA-Ethernet1/0/1] port link-type hybrid
```

Configure the voice VLAN as the default VLAN of Ethernet 1/0/1, and add the voice VLAN to the list of untagged VLANs whose traffic is permitted by the port.

```
[DeviceA-Ethernet1/0/1] port hybrid pvid vlan 2
[DeviceA-Ethernet1/0/1] port hybrid vlan 2 untagged
```

Enable the voice VLAN function on Ethernet 1/0/1.

```
[DeviceA-Ethernet1/0/1] voice vlan enable
```

Verification

Display the OUI addresses, the corresponding OUI address masks and the corresponding description strings that the system supports.

```
<DeviceA> display voice vlan oui
Oui Address     Mask            Description
0003-6b00-0000  ffff-ff00-0000  Cisco phone
000f-e200-0000  ffff-ff00-0000  H3C Aolynk phone
0011-2200-0000  ffff-ff00-0000  test
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3Com phone
```

Display the status of the current voice VLAN.

```
<DeviceA> display voice vlan status
Voice Vlan status: ENABLE
Voice Vlan ID: 2
Voice Vlan security mode: Security
Voice Vlan aging time: 1440 minutes
Current voice vlan enabled port mode:
PORT                      MODE
-------------------------------
Ethernet1/0/1             MANUAL
```

Table of Contents

1 Port Basic Configuration

When performing basic port configuration, go to these sections for information you are interested in:

- Ethernet Port Configuration
- Ethernet Port Configuration Example
- Troubleshooting Ethernet Port Configuration

Ethernet Port Configuration

Combo Port Configuration

Introduction to Combo port

A Combo port can operate as either an optical port or an electrical port. Inside the device there is only one forwarding interface. For a Combo port, the electrical port and the corresponding optical port are TX-SFP multiplexed. You can specify a Combo port to operate as an electrical port or an optical port. That is, a Combo port cannot operate as both an electrical port and an optical port simultaneously. When one is enabled, the other is automatically disabled.

Configuring Combo port state

Follow these steps to configure the state of a Combo port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable a specified Combo port	**undo shutdown**	Optional By default, of the two ports in a Combo port, the one with a smaller port ID is enabled.

Note

In case of a Combo port, only one interface (either the optical port or the electrical port) is active at a time. That is, once the optical port is active, the electrical port will be inactive automatically, and vice versa.

Initially Configuring a Port

Follow these steps to initially configure a port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the Ethernet port	**undo shutdown**	Optional By default, the port is enabled. Use the **shutdown** command to disable the port.
Set the description string for the Ethernet port	**description** *text*	Optional By default, the description string of an Ethernet port is null.
Set the duplex mode of the Ethernet port	**duplex** { **auto** | **full** | **half** }	Optional By default, the duplex mode of the port is **auto** (auto-negotiation).
Set the speed of the Ethernet port	**speed** { **10** | **100** | **1000** | **auto** }	Optional • By default, the speed of an Ethernet port is determined through auto-negotiation (the auto keyword). • Use the 1000 keyword for Gigabit Ethernet ports only.
Set the medium dependent interface (MDI) mode of the Ethernet port	**mdi** { **across** | **auto** | **normal** }	Optional Be default, the MDI mode of an Ethernet port is **auto**.
Set the maximum frame size allowed on the Ethernet port to 9,216 bytes	**jumboframe enable**	Optional By default, the maximum frame size allowed on an Ethernet is 9,216 bytes. To set the maximum frame size allowed on an Ethernet port to 1,522 bytes, use the **undo jumboframe enable** command.

Configuring Port Auto-Negotiation Speed

You can configure an auto-negotiation speed for a port by using the **speed auto** command.

Take a 10/100/1000 Mbps port as an example.

- If you expect that 10 Mbps is the only available auto-negotiation speed of the port, you just need to configure **speed auto 10**.
- If you expect that 10 Mbps and 100 Mbps are the available auto-negotiation speeds of the port, you just need to configure **speed auto 10 100**.
- If you expect that 10 Mbps and 1000 Mbps are the available auto-negotiation speeds of the port, you just need to configure **speed auto 10 1000**.

Follow these steps to configure auto-negotiation speeds for a port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet interface view	**interface** *interface-type interface-number*	—
Configure the available auto-negotiation speed(s) for the port	**speed auto** [**10** | **100** | **1000**]*	Optional • By default, the port speed is determined through auto-negotiation. • Use the **1000** keyword for Gigabit Ethernet ports only.

Note

- Only ports on the front panel of the device support the auto-negotiation speed configuration feature. And ports on the extended interface card do not support this feature currently.
- After you configure auto-negotiation speed(s) for a port, if you execute the **undo speed** command or the **speed auto** command, the auto-negotiation speed setting of the port restores to the default setting.
- The effect of executing **speed auto 10 100 1000** equals to that of executing **speed auto**, that is, the port is configured to support all the auto-negotiation speeds: 10 Mbps, 100 Mbps, and 1000 Mbps.

Limiting Traffic on individual Ports

By performing the following configurations, you can limit the incoming broadcast/multicast/unknown unicast traffic on individual ports. When a type of incoming traffic exceeds the threshold you set, the system drops the packets exceeding the traffic limit to reduce the traffic ratio of this type to the reasonable range, so as to keep normal network service.

Follow these steps to limit traffic on port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Limit broadcast traffic received on each port	**broadcast-suppression** { *ratio* | **pps** *max-pps* }	Optional By default, the switch does not suppress broadcast traffic.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Limit broadcast traffic received on the current port	**broadcast-suppression** { *ratio* | **pps** *max-pps* }	Optional By default, the switch does not suppress broadcast traffic.
Limit multicast traffic received on the current port	**multicast-suppression** { *ratio* | **pps** *max-pps* }	Optional By default, the switch does not suppress multicast traffic.

To do...	Use the command...	Remarks
Limit unknown unicast traffic received on the current port	**unicast-suppression** { *ratio* | **pps** *max-pps* }	Optional By default, the switch does not suppress unknown unicast traffic.

Enabling Flow Control on a Port

Flow control is enabled on both the local and peer switches. If congestion occurs on the local switch:

- The local switch sends a message to notify the peer switch of stopping sending packets to itself or reducing the sending rate temporarily.
- The peer switch will stop sending packets to the local switch or reduce the sending rate temporarily when it receives the message; and vice versa. By this way, packet loss is avoided and the network service operates normally.

Follow these steps to enable flow control on a port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable flow control on the Ethernet port	**flow-control**	By default, flow control is not enabled on the port.

Duplicating the Configuration of a Port to Other Ports

To make other ports have the same configuration as that of a specific port, you can duplicate the configuration of a port to specific ports.

Specifically, the following types of port configuration can be duplicated from one port to other ports: VLAN configuration, LACP configuration, QoS configuration, STP configuration and initial port configuration. Refer to the command manual for the configurations that can be duplicated.

Follow these steps to duplicate the configuration of a port to specific ports:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Duplicate the configuration of a port to specific ports	**copy configuration source** { *interface-type interface-number* | **aggregation-group** *source-agg-id* } **destination** { *interface-list* [**aggregation-group** *destination-agg-id*] | **aggregation-group** *destination-agg-id* }	Required

Note

- If you specify a source aggregation group ID, the system will use the port with the smallest port number in the aggregation group as the source.
- If you specify a destination aggregation group ID, the configuration of the source port will be copied to all ports in the aggregation group and all ports in the group will have the same configuration as that of the source port.

Configuring Loopback Detection for an Ethernet Port

Loopback detection is used to monitor if loopback occurs on a switch port.

After you enable loopback detection on Ethernet ports, the switch can monitor if external loopback occurs on them. If there is a loopback port found, the switch will put it under control.

- If loopback is found on an access port, the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.
- If loopback is found on a trunk or hybrid port, the system sends a Trap message to the client. When the loopback port control function is enabled on these ports, the system disables the port, sends a Trap message to the client and removes the corresponding MAC forwarding entry.

Follow these steps to configure loopback detection for an Ethernet port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable loopback detection globally	**loopback-detection enable**	Required By default, loopback detection is disabled globally.
Set the interval for performing port loopback detection	**loopback-detection interval-time** *time*	Optional The default is 30 seconds.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable loopback detection on a specified port	**loopback-detection enable**	Required By default, port loopback detection is disabled.
Enable loopback port control on the trunk or hybrid port	**loopback-detection control enable**	Optional By default, loopback port control is not enabled.
Configure the system to run loopback detection on all VLANs of the current trunk or hybrid port	**loopback-detection per-vlan enable**	Optional By default, the system runs loopback detection only on the default VLAN of the current trunk or hybrid port.

Caution

- To enable loopback detection on a specific port, you must use the **loopback-detection enable** command in both system view and the specific port view.
- After you use the **undo loopback-detection enable** command in system view, loopback detection will be disabled on all ports.

Enabling Loopback Test

You can configure the Ethernet port to run loopback test to check if it operates normally. The port running loopback test cannot forward data packets normally. The loopback test terminates automatically after a specific period.

Follow these steps to enable loopback test:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable loopback test	**loopback** { **external** | **internal** }	Required

Note

- **external**: Performs external loop test. In the external loop test, self-loop headers must be used on the port of the switch (for 100M port, the self-loop headers are made from four cores of the 8-core cables, for 1000M port, the self-loop header are made from eight cores of the 8-core cables, then the packets forwarded by the port will be received by itself.). The external loop test can locate the hardware failures on the port.
- **internal**: Performs internal loop test. In the internal loop test, self loop is established in the switching chip to locate the chip failure which is related to the port.

Note that:

- After you use the **shutdown** command on a port, the port cannot run loopback test.
- You cannot use the **speed**, **duplex**, **mdi** and **shutdown** commands on the ports running loopback test.
- Some ports do not support loopback test, and corresponding prompts will be given when you perform loopback test on them.

Enabling the System to Test Connected Cable

You can enable the system to test the cable connected to a specific port. The test result will be returned in five seconds. The system can test these attributes of the cable: Receive and transmit directions (RX and TX), short circuit/open circuit or not, the length of the faulty cable.

Follow these steps to enable the system to test connected cables:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the system to test connected cables	**virtual-cable-test**	Required

Configuring the Interval to Perform Statistical Analysis on Port Traffic

By performing the following configuration, you can set the interval to perform statistical analysis on the traffic of a port.

When you use the **display interface** *interface-type interface-number* command to display the information of a port, the system performs statistical analysis on the traffic flow passing through the port during the specified interval and displays the average rates in the interval. For example, if you set this interval to 100 seconds, the displayed information is as follows:

```
Last 100 seconds input:  0 packets/sec 0 bytes/sec
Last 100 seconds output:  0 packets/sec 0 bytes/sec
```

Follow these steps to set the interval to perform statistical analysis on port traffic:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the interval to perform statistical analysis on port traffic	**flow-interval** *interval*	Optional By default, this interval is 300 seconds.

Enabling Giant-Frame Statistics Function

The giant-frame statistics function is used to ensure normal data transmission and to facilitate statistics and analysis of unusual traffic on the network.

Follow these steps to enable the giant-frame statistics function:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable the giant-frame statistics function	**giant-frame statistics enable**	Required By default, the giant-frame statistics function is not enabled.

Setting the Port State Change Delay

During a short period after you connect your switch to another device, the connecting port may go up and down frequently due to hardware compatibility, resulting in service interruption.

To avoid situations like this, you may introduce a port state change delay.

Caution

The port state change delay takes effect when the port goes down but not when the port goes up.

Follow these steps to set the port state change delay:

To do …	Use the command …	Remarks
Enter system view	**system-view**	—
Enter Ethernet interface view	**interface** *interface-type interface-number*	—
Set the port state change delay	**link-delay** *delay-time*	Required Defaults to 0, which indicates that no delay is introduced.

Note

The delay configured in this way does not take effect for ports in DLDP down state. For information about the DLDP down state, refer to *DLDP*.

Displaying and Maintaining Basic Port Configuration

To do...	Use the command...	Remarks
Display port configuration information	**display interface** [*interface-type* | *interface-type interface-number*]	Available in any view
Display the enable/disable status of port loopback detection	**display loopback-detection**	
Display brief information about port configuration	**display brief interface** [*interface-type* [*interface-number*]] [**|** { **begin** | **include** | **exclude** } *regular-expression*]	
Display port information about a specified unit	**display unit** *unit-id* **interface**	
Display the Combo ports and the corresponding optical/electrical ports	**display port combo**	
Display the information about the port with the **link-delay** command configured	**display link-delay**	

To do...	Use the command...	Remarks
Clear port statistics	**reset counters interface** [*interface-type* | *interface-type interface-number*]	Available in user view After 802.1x is enabled on a port, clearing the statistics on the port will not work.

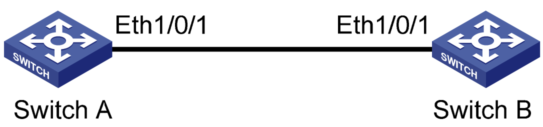
Ethernet Port Configuration Example

Network requirements

- Switch A and Switch B are connected to each other through two trunk port (Ethernet 1/0/1).
- Configure the default VLAN ID of both Ethernet 1/0/1 to 100.
- Allow the packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass both Ethernet 1/0/1.

Network diagram

Figure 1-1 Network diagram for Ethernet port configuration



Configuration procedure

Note

- Only the configuration for Switch A is listed below. The configuration for Switch B is similar to that of Switch A.
- This example supposes that VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 have been created.

Enter Ethernet 1/0/1 port view.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0/1
```

Set Ethernet 1/0/1 as a trunk port.

```
[Sysname-Ethernet1/0/1] port link-type trunk
```

Allow packets of VLAN 2, VLAN 6 through VLAN 50 and VLAN 100 to pass Ethernet 1/0/1.

```
[Sysname-Ethernet1/0/1] port trunk permit vlan 2 6 to 50 100
```

Configure the default VLAN ID of Ethernet 1/0/1 to 100.

```
[Sysname-Ethernet1/0/1] port trunk pvid vlan 100
```

Troubleshooting Ethernet Port Configuration

Symptom: Fail to configure the default VLAN ID of an Ethernet port.

Solution: Take the following steps:

- Use the **display interface** or **display port** command to check if the port is a trunk port or a hybrid port.
- If the port is not a trunk or hybrid port, configure it to be a trunk or hybrid port.
- Configure the default VLAN ID of the port.

Table of Contents

1 Link Aggregation Configuration

When configuring link aggregation, go to these sections for information you are interested in:

- Overview
- Link Aggregation Classification
- Aggregation Group Categories
- Link Aggregation Configuration
- Displaying and Maintaining Link Aggregation Configuration
- Link Aggregation Configuration Example

Overview

Introduction to Link Aggregation

Link aggregation aggregates multiple physical Ethernet ports into one logical link, also called an aggregation group.

It allows you to increase bandwidth by distributing traffic across the member ports in the aggregation group. In addition, it provides reliable connectivity because these member ports can dynamically back up each other.

Introduction to LACP

The Link Aggregation Control Protocol (LACP) is defined in IEEE 802.3ad. It uses link aggregation control protocol data units (LACPDUs) for information exchange between LACP-enabled devices.

With LACP enabled on a port, LACP notifies the following information of the port to its peer by sending LACPDUs: priority and MAC address of this system, priority, number and operation key of the port. Upon receiving the information, the peer compares the information with the information of other ports on the peer device to determine the ports that can be aggregated. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group.

When aggregating ports, link aggregation control automatically assigns each port an operational key based on the port speed, duplex mode, and basic configurations described in Consistency Considerations for the Ports in Aggregation.

In a manual or static link aggregation group, the selected ports are assigned the same operational key. In a dynamic link aggregation group, all member ports are assigned the same operational key.

Consistency Considerations for the Ports in Aggregation

To participate in traffic sharing, member ports in an aggregation group must use the same configurations with respect to STP, QoS, QinQ, VLAN, port attributes and so on as shown in the following table.

Table 1-1 Consistency considerations for ports in an aggregation

Category	Considerations
STP	State of port-level STP (enabled or disabled) Attribute of the link (point-to-point or otherwise) connected to the port Port path cost STP priority STP packet format Loop protection Root protection Port type (whether the port is an edge port)
QoS	Rate limiting Priority marking 802.1p priority Traffic redirecting
Link type	Link type of the ports (trunk, hybrid, or access)
VLAN-VPN	State of VLAN-VPN (enabled or disabled) TPID on the ports State of inner-to-outer tag priority replication (enabled or disabled)

Note

The Switch 4500 family support cross-device link aggregation if XRN fabric is enabled.

Link Aggregation Classification

Depending on different aggregation modes, the following three types of link aggregation exist:

- Manual aggregation
- Static LACP aggregation
- Dynamic LACP aggregation

Manual Aggregation Group

Introduction to manual aggregation group

A manual aggregation group is manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each manual aggregation group must contain at least one port. When a manual aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

LACP is disabled on the member ports of manual aggregation groups, and you cannot enable LACP on ports in a manual aggregation group.

Port status in manual aggregation group

A port in a manual aggregation group can be in one of the two states: selected or unselected. In a manual aggregation group, only the selected ports can forward user service packets.

In a manual aggregation group, the system sets the ports to selected or unselected state according to the following rules.

- Among the ports in an aggregation group that are in up state, the system determines the mater port with one of the following settings being the highest (in descending order) as the master port: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The ports with their rate, duplex mode and link type being the same as that of the master port are selected ports, and the rest are unselected ports.
- There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the selected ports in an aggregation group exceeds the maximum number supported by the device, those with lower port numbers operate as the selected ports, and others as unselected ports.

Among the selected ports in an aggregation group, the one with smallest port number operates as the master port. Other selected ports are the member ports.

Requirements on ports for manual aggregation

Generally, there is no limit on the rate and duplex mode of the ports (also including initially down port) you want to add to a manual aggregation group.

Static LACP Aggregation Group

Introduction to static LACP aggregation

A static LACP aggregation group is also manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each static aggregation group must contain at least one port. When a static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

LACP is enabled on the member ports of static aggregation groups. When you remove a static aggregation group, all the member ports in up state form one or multiple dynamic aggregations with LACP enabled. LACP cannot be disabled on static aggregation ports.

Port status of static aggregation group

A port in a static aggregation group can be in one of the two states: selected or unselected.

- Both the selected and the unselected ports in the up state can transceive LACP protocol packets.
- Only the selected ports can transceive service packets; the unselected ports cannot.

In a static aggregation group, the system sets the ports to selected or unselected state according to the following rules.

- Among the ports in an aggregation group that are in up state, the system determines the master port with one of the following settings being the highest (in descending order) as the master port: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The ports with their rate, duplex mode and link type being the same as that of the master port are selected port, and the rest are unselected ports.
- The ports connected to a peer device different from the one the master port is connected to or those connected to the same peer device as the master port but to a peer port that is not in the same aggregation group as the peer port of the master port are unselected ports.
- The system sets the ports with basic port configuration different from that of the master port to unselected state.

- There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the selected ports in an aggregation group exceeds the maximum number supported by the device, those with lower port numbers operate as the selected ports, and others as unselected ports.

Dynamic LACP Aggregation Group

Introduction to dynamic LACP aggregation group

A dynamic LACP aggregation group is automatically created and removed by the system. Users cannot add/remove ports to/from it. Ports can be aggregated into a dynamic aggregation group only when they are connected to the same peer device and have the same speed, duplex mode, and basic configurations, and their peer ports have the same configurations.

Besides multiple-port aggregation groups, the system is also able to create single-port aggregation groups, each of which contains only one port. LACP is enabled on the member ports of dynamic aggregation groups.

Port status of dynamic aggregation group

A port in a dynamic aggregation group can be in one of the two states: selected and unselected.

- Both the selected and the unselected ports can receive/transmit LACP protocol packets;
- The selected ports can receive/transmit user service packets, but the unselected ports cannot.
- In a dynamic aggregation group, the selected port with the smallest port number serves as the master port of the group, and other selected ports serve as member ports of the group.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports that can be set as selected ports in an aggregation group exceeds the maximum number supported by the device, the system will negotiate with its peer end, to determine the states of the member ports according to the port IDs of the preferred device (that is, the device with smaller system ID). The following is the negotiation procedure:

1) Compare device IDs (system priority + system MAC address) between the two parties. First compare the two system priorities, then the two system MAC addresses if the system priorities are equal. The device with smaller device ID will be considered as the preferred one.
2) Compare port IDs (port priority + port number) on the preferred device. The comparison between two port IDs is as follows: First compare the two port priorities, then the two port numbers if the two port priorities are equal; the port with the smallest port ID is the selected port and the left ports are unselected ports.

Note

For an aggregation group:

- When the rate or duplex mode of a port in the aggregation group changes, packet loss may occur on this port;
- When the rate of a port decreases, if the port belongs to a manual or static LACP aggregation group, the port will be switched to the unselected state; if the port belongs to a dynamic LACP aggregation group, deaggregation will occur on the port.

Aggregation Group Categories

Depending on whether or not load sharing is implemented, aggregation groups can be load-sharing or non-load-sharing aggregation groups. When load sharing is implemented,

- For IP packets, the system will implement load-sharing based on source IP address and destination IP address;
- For non-IP packets, the system will implement load-sharing based on source MAC address and destination MAC address.

In general, the system only provides limited load-sharing aggregation resources, so the system needs to reasonably allocate the resources among different aggregation groups.

The system always allocates hardware aggregation resources to the aggregation groups with higher priorities. When load-sharing aggregation resources are used up by existing aggregation groups, newly-created aggregation groups will be non-load-sharing ones.

Load-sharing aggregation resources are allocated to aggregation groups in the following order:

- An aggregation group containing special ports which require hardware aggregation resources has higher priority than any aggregation group containing no special port.
- A manual or static aggregation group has higher priority than a dynamic aggregation group (unless the latter contains special ports while the former does not).
- For aggregation groups, the one that might gain higher speed if resources were allocated to it has higher priority than others. If the groups can gain the same speed, the one with smallest master port number has higher priority than other groups.

When an aggregation group of higher priority appears, the aggregation groups of lower priorities release their hardware resources. For single-port aggregation groups, they can transceive packets normally without occupying aggregation resources

---

Caution

- A load-sharing aggregation group contains at least two selected ports, but a non-load-sharing aggregation group can only have one selected port at most, while others are unselected ports.
- When more than eight load-sharing aggregation groups are configured on a single switch, fabric ports cannot be enabled on this switch.
- When no more than eight load-sharing aggregation groups are configured on a single switch, fabric ports can be enabled on this switch. The aggregation groups added subsequently are all non-load-sharing aggregation groups. If the fabric ports are disabled, the state of these non-load-sharing aggregation groups will not be changed automatically. These non-load-sharing aggregation groups will become load-sharing aggregation groups only after the unselected ports in these aggregation groups are unplugged and then plugged or the **shutdown** command and then the **undo shutdown** command are executed.

Link Aggregation Configuration

Caution

- The commands of link aggregation cannot be configured with the commands of port loopback detection feature at the same time.
- The ports where the **mac-address max-mac-count** command is configured cannot be added to an aggregation group. Contrarily, the **mac-address max-mac-count** command cannot be configured on a port that has already been added to an aggregation group.
- MAC-authentication-enabled ports and 802.1x-enabled ports cannot be added to an aggregation group.
- Mirroring destination ports and mirroring reflector ports cannot be added to an aggregation group.
- Ports configured with blackhole MAC addresses, static MAC addresses, multicast MAC addresses, or the static ARP protocol cannot be added to an aggregation group.
- Port-security-enabled ports cannot be added to an aggregation group.
- The port with Voice VLAN enabled cannot be added to an aggregation group.
- Do not add ports with the inter-VLAN MAC address replicating function of the selective QinQ feature enabled to an aggregation group.

Configuring a Manual Aggregation Group

You can create a manual aggregation group, or remove an existing manual aggregation group (after that, all the member ports will be removed from the group).

For a manual aggregation group, a port can only be manually added/removed to/from the manual aggregation group.

Follow these steps to configure a manual aggregation group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a manual aggregation group	**link-aggregation group** *agg-id* **mode manual**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add the Ethernet port to the aggregation group	**port link-aggregation group** *agg-id*	Required

Note that:

1) When creating an aggregation group:

- If the aggregation group you are creating already exists but contains no port, its type will change to the type you set.
- If the aggregation group you are creating already exists and contains ports, the possible type changes may be: changing from dynamic or static to manual, and changing from dynamic to static; and no other kinds of type change can occur.

- When you change a dynamic/static group to a manual group, the system will automatically disable LACP on the member ports. When you change a dynamic group to a static group, the system will remain the member ports LACP-enabled.

2) When a manual or static aggregation group contains only one port, you cannot remove the port unless you remove the whole aggregation group.

Configuring a Static LACP Aggregation Group

You can create a static LACP aggregation group, or remove an existing static LACP aggregation group (after that, the system will re-aggregate the original member ports in the group to form one or multiple dynamic aggregation groups.).

For a static aggregation group, a port can only be manually added/removed to/from the static aggregation group.

Note

When you add an LACP-enabled port to a manual aggregation group, the system will automatically disable LACP on the port. Similarly, when you add an LACP-disabled port to a static aggregation group, the system will automatically enable LACP on the port.

Follow these steps to configure a static LACP aggregation group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a static aggregation group	**link-aggregation group** *agg-id* **mode static**	Required
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add the port to the aggregation group	**port link-aggregation group** *agg-id*	Required

Note

For a static LACP aggregation group or a manual aggregation group, you are recommended not to cross cables between the two devices at the two ends of the aggregation group. For example, suppose port 1 of the local device is connected to port 2 of the peer device. To avoid cross-connecting cables, do not connect port 2 of the local device to port 1 of the peer device. Otherwise, packets may be lost.

Configuring a Dynamic LACP Aggregation Group

A dynamic LACP aggregation group is automatically created by the system based on LACP-enabled ports. The adding and removing of ports to/from a dynamic aggregation group are automatically accomplished by LACP.

You need to enable LACP on the ports which you want to participate in dynamic aggregation of the system, because, only when LACP is enabled on those ports at both ends, can the two parties reach agreement in adding/removing ports to/from dynamic aggregation groups.

Note

You cannot enable LACP on a port which is already in a manual aggregation group.

Follow these steps to configure a dynamic LACP aggregation group:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the system priority	**lacp system-priority** *system-priority*	Optional By default, the system priority is 32,768.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable LACP on the port	**lacp enable**	Required By default, LACP is disabled on a port.
Configure the port priority	**lacp port-priority** *port-priority*	Optional By default, the port priority is 32,768.

Note

Changing the system priority may affect the priority relationship between the aggregation peers, and thus affect the selected/unselected status of member ports in the dynamic aggregation group.

Configuring a Description for an Aggregation Group

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a description for an aggregation group	**link-aggregation group** *agg-id* **description** *agg-name*	Optional By default, no description is configured for an aggregation group.

Caution

If you have saved the current configuration with the **save** command, after system reboot, the configuration concerning manual and static aggregation groups and their descriptions still exists, but that of dynamic aggregation groups and their descriptions gets lost.

Displaying and Maintaining Link Aggregation Configuration

To do…	Use the command…	Remarks
Display summary information of all aggregation groups	**display link-aggregation summary**	Available in any view
Display detailed information of a specific aggregation group or all aggregation groups	**display link-aggregation verbose** [*agg-id*]	
Display link aggregation details of a specified port or port range	**display link-aggregation interface** *interface-type interface-number* [**to** *interface-type interface-number*]	
Display local device ID	**display lacp system-id**	
Clear LACP statistics about a specified port or port range	**reset lacp statistics** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]	Available in user view

Link Aggregation Configuration Example

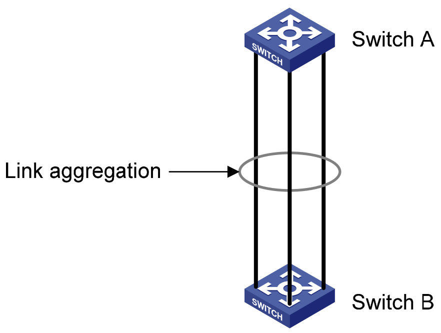
Ethernet Port Aggregation Configuration Example

Network requirements

- Switch A connects to Switch B with three ports Ethernet 1/0/1 to Ethernet 1/0/3. It is required that load between the two switches can be shared among the three ports.
- Adopt three different aggregation modes to implement link aggregation on the three ports between switch A and B.

Network diagram

Figure 1-1 Network diagram for link aggregation configuration



Configuration procedure

Note

The following only lists the configuration on Switch A; you must perform the similar configuration on Switch B to implement link aggregation.

---

1) Adopting manual aggregation mode

\# Create manual aggregation group 1.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode manual
```

\# Add Ethernet 1/0/1 through Ethernet 1/0/3 to aggregation group 1.

```
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] port link-aggregation group 1
[Sysname-Ethernet1/0/1] quit
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] port link-aggregation group 1
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet1/0/3
[Sysname-Ethernet1/0/3] port link-aggregation group 1
```

2) Adopting static LACP aggregation mode

\# Create static aggregation group 1.

```
<Sysname> system-view
[Sysname] link-aggregation group 1 mode static
```

\# Add Ethernet 1/0/1 through Ethernet 1/0/3 to aggregation group 1.

```
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] port link-aggregation group 1
[Sysname-Ethernet1/0/1] quit
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] port link-aggregation group 1
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet1/0/3
[Sysname-Ethernet1/0/3] port link-aggregation group 1
```

3) Adopting dynamic LACP aggregation mode

\# Enable LACP on Ethernet 1/0/1 through Ethernet 1/0/3.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] lacp enable
[Sysname-Ethernet1/0/1] quit
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] lacp enable
[Sysname-Ethernet1/0/2] quit
```

```
[Sysname] interface Ethernet1/0/3
[Sysname-Ethernet1/0/3] lacp enable
```

Caution

The three LACP-enabled ports can be aggregated into one dynamic aggregation group to implement load sharing only when they have the same basic configuration (such as rate, duplex mode, and so on).

Table of Contents

1 Port Isolation Configuration

When configuring port isolation, go to these sections for information you are interested in:

- Port Isolation Overview
- Port Isolation Configuration
- Displaying and Maintaining Port Isolation Configuration
- Port Isolation Configuration Example

Port Isolation Overview

The port isolation feature is used to secure and add privacy to the data traffic and prevent malicious attackers from obtaining the user information. With the port isolation feature, you can add the ports to be controlled into an isolation group to isolate the Layer 2 and Layer 3 data between each port in the isolation group (a port in an isolation group does not forward traffic to the other ports in the isolation group).

The ports in an isolation group must reside on the same switch or different units of an XRN fabric.

Note

- Currently, you can create only on isolation group on a Switch 4500 series switch. The number of Ethernet ports in an isolation group is not limited.
- An isolation group only isolates the member ports in it.

Port Isolation Configuration

You can perform the following operations to add an Ethernet port to an isolation group, thus isolating Layer 2 and Layer 3 data among the ports in the isolation group.

Follow these steps to configure port isolation:

To do …	Use the command …	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add the Ethernet port to the isolation group	**port isolate**	Required By default, an isolation group contains no port.

Note

- When a member port of an aggregation group joins/leaves an isolation group, the other ports in the same aggregation group will join/leave the isolation group at the same time.
- For ports that belong to an aggregation group and an isolation group simultaneously, removing a port from the aggregation group has no effect on the other ports. That is, the rest ports remain in the aggregation group and the isolation group.
- Ports that belong to an aggregation group and an isolation group simultaneously are still isolated even when you remove the aggregation group in system view.
- Adding an isolated port to an aggregation group causes all the ports in the aggregation group on the local unit to be added to the isolation group.
- Switch 4500 series switches support cross-device port isolation if XRN fabric is enabled.
- For Switch 4500 series switches belonging to the same XRN Fabric, the port isolation configuration performed on a port of a cross-device aggregation group cannot be synchronized to the other ports of the aggregation group if the ports reside on other units. That is, to add multiple ports in a cross-device aggregation group to the same isolation group, you need to perform the configuration for each of the ports individually.

Displaying and Maintaining Port Isolation Configuration

To do …	Use the command …	Remarks
Display information about the Ethernet ports added to the isolation group	**display isolate port**	Available in any view

Port Isolation Configuration Example

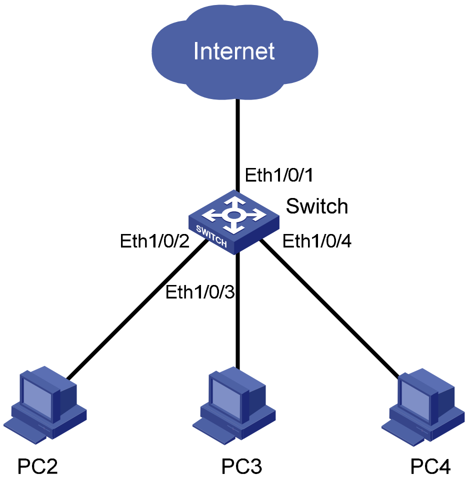
Network requirements

As shown in Figure 1-1, PC2, PC3 and PC4 connect to the switch ports Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 respectively. The switch connects to the Internet through Ethernet1/0/1.

It is desired to isolate PC2, PC3 and PC4 to disable them from communicating directly with each other.

Network diagram

Figure 1-1 Network diagram for port isolation configuration



Configuration procedure

Add Ethernet1/0/2, Ethernet1/0/3, and Ethernet1/0/4 to the isolation group.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] interface ethernet1/0/2
[Sysname-Ethernet1/0/2] port isolate
[Sysname-Ethernet1/0/2] quit
[Sysname] interface ethernet1/0/3
[Sysname-Ethernet1/0/3] port isolate
[Sysname-Ethernet1/0/3] quit
[Sysname] interface ethernet1/0/4
[Sysname-Ethernet1/0/4] port isolate
[Sysname-Ethernet1/0/4] quit
[Sysname] quit
```

Display information about the ports in the isolation group.

```
<Sysname> display isolate port
 Isolated port(s) on UNIT 1:
 Ethernet1/0/2, Ethernet1/0/3, Ethernet1/0/4
```

Table of Contents

1 Port Security Configuration

When configuring port security, go to these sections for information you are interested in:

- Port Security Overview
- Port Security Configuration Task List
- Displaying and Maintaining Port Security Configuration
- Port Security Configuration Examples

Port Security Overview

Introduction

Port security is a security mechanism for network access control. It is an expansion to the current 802.1x and MAC address authentication.

Port security allows you to define various security modes that enable devices to learn legal source MAC addresses, so that you can implement different network security management as needed.

With port security enabled, packets whose source MAC addresses cannot be learned by your switch in a security mode are considered illegal packets, The events that cannot pass 802.1x authentication or MAC authentication are considered illegal.

With port security enabled, upon detecting an illegal packet or illegal event, the system triggers the corresponding port security features and takes pre-defined actions automatically. This reduces your maintenance workload and greatly enhances system security and manageability.

Port Security Features

The following port security features are provided:

- NTK (need to know) feature: By checking the destination MAC addresses in outbound data frames on the port, NTK ensures that the switch sends data frames through the port only to successfully authenticated devices, thus preventing illegal devices from intercepting network data.
- Intrusion protection feature: By checking the source MAC addresses in inbound data frames or the username and password in 802.1x authentication requests on the port, intrusion protection detects illegal packets or events and takes a pre-set action accordingly. The actions you can set include: disconnecting the port temporarily/permanently, and blocking packets with the MAC address specified as illegal.
- Trap feature: When special data packets (generated from illegal intrusion, abnormal login/logout or other special activities) are passing through the switch port, Trap feature enables the switch to send Trap messages to help the network administrator monitor special activities.

Port Security Modes

Table 1-1 describes the available port security modes:

Table 1-1 Description of port security modes

Security mode	Description	Feature
noRestriction	In this mode, access to the port is not restricted.	In this mode, neither the NTK nor the intrusion protection feature is triggered.
autolearn	In this mode, a port can learn a specified number of MAC addresses and save those addresses as security MAC addresses. It permits only packets whose source MAC addresses are the security MAC addresses that were learned or configured manually. When the number of security MAC addresses reaches the upper limit configured by the **port-security max-count** command, the port changes to work in **secure** mode and no more MAC addresses can be added to the port.	In either mode, the device will trigger NTK and intrusion protection upon detecting an illegal packet.
secure	In this mode, MAC address learning is disabled on the port. The port permits packets whose source MAC addresses are static and dynamic MAC addresses that were configured manually. When the port mode changes from **autolearn** to **secure**, the security MAC addresses that were learned in the **autolearn** mode are permitted to pass through the port.	

<table>
<tr><th>Security mode</th><th>Description</th><th>Feature</th></tr>
<tr><td>userlogin</td><td>In this mode, port-based 802.1x authentication is performed for access users.</td><td>In this mode, neither NTK nor intrusion protection will be triggered.</td></tr>
<tr><td>userLoginSecure</td><td>MAC-based 802.1x authentication is performed on the access user. The port is enabled only after the authentication succeeds. When the port is enabled, only the packets of the successfully authenticated user can pass through the port.
In this mode, only one 802.1x-authenticated user is allowed to access the port.
When the port changes from the noRestriction mode to this security mode, the system automatically removes the existing dynamic MAC address entries and authenticated MAC address entries on the port.</td><td rowspan="6">In any of these modes, the device triggers the NTK and Intrusion Protection features upon detecting an illegal packet or illegal event.</td></tr>
<tr><td>userLoginSecureExt</td><td>This mode is similar to the userLoginSecure mode, except that there can be more than one 802.1x-authenticated user on the port.</td></tr>
<tr><td>userLoginWithOUI</td><td>This mode is similar to the userLoginSecure mode, except that, besides the packets of the single 802.1x-authenticated user, the packets whose source MAC addresses have a particular OUI are also allowed to pass through the port.
When the port changes from the normal mode to this security mode, the system automatically removes the existing dynamic/authenticated MAC address entries on the port.</td></tr>
<tr><td>macAddressWithRadius</td><td>In this mode, MAC address–based authentication is performed for access users.</td></tr>
<tr><td>macAddressOrUserLoginSecure</td><td>In this mode, both MAC authentication and 802.1x authentication can be performed, but 802.1x authentication has a higher priority.
802.1x authentication can still be performed on an access user who has passed MAC authentication.
No MAC authentication is performed on an access user who has passed 802.1x authentication.
In this mode, there can be only one 802.1x-authenticated user on the port, but there can be several MAC-authenticated users.</td></tr>
<tr><td>macAddressOrUserLoginSecureExt</td><td>This mode is similar to the macAddressOrUserLoginSecure mode, except that there can be more than one 802.1x-authenticated user on the port. .</td></tr>
</table>

Security mode	Description	Feature
macAddressElseUserLoginSecure	In this mode, a port performs MAC authentication of an access user first. If the authentication succeeds, the user is authenticated. Otherwise, the port performs 802.1x authentication of the user. In this mode, there can be only one 802.1x-authenticated user on the port, but there can be several MAC-authenticated users.	
macAddressElseUserLoginSecureExt	This mode is similar to the **macAddressElseUserLoginSecure** mode, except that there can be more than one 802.1x-authenticated user on the port.	
macAddressAndUserLoginSecure	In this mode, a port firstly performs MAC authentication for a user and then performs 802.1x authentication for the user if the user passes MAC authentication. The user can access the network after passing the two authentications. In this mode, up to one user can access the network.	
macAddressAndUserLoginSecureExt	This mode is similar to the **macAddressAndUserLoginSecure** mode, except that more than one user can access the network.	

Note

- When the port operates in the **userlogin-withoui** mode, Intrusion Protection will not be triggered even if the OUI address does not match.
- On a port operating in either the **macAddressElseUserLoginSecure** mode or the **macAddressElseUserLoginSecureExt** mode, Intrusion Protection is triggered only after both MAC-based authentication and 802.1x authentication on the same packet fail.

Port Security Configuration Task List

Complete the following tasks to configure port security:

Task		Remarks
Enabling Port Security		Required
Setting the Maximum Number of MAC Addresses Allowed on a Port		Optional
Setting the Port Security Mode		Required
Configuring Port Security Features	Configuring the NTK feature	Optional Choose one or more features as required.
	Configuring intrusion protection	
	Configuring the Trap feature	
Ignoring the Authorization Information from the RADIUS Server		Optional

Task	Remarks
Configuring Security MAC Addresses	Optional

Enabling Port Security

Configuration Prerequisites

Before enabling port security, you need to disable 802.1x and MAC authentication globally.

Enabling Port Security

Follow these steps to enable port security:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable port security	**port-security enable**	Required Disabled by default

Caution

Enabling port security resets the following configurations on the ports to the defaults (shown in parentheses below):

- 802.1x (disabled), port access control method (**macbased**), and port access control mode (**auto**)
- MAC authentication (disabled)

In addition, you cannot perform the above-mentioned configurations manually because these configurations change with the port security mode automatically.

Note

- For details about 802.1x configuration, refer to the sections covering 802.1x and System-Guard.
- For details about MAC authentication configuration, refer to the sections covering MAC authentication configuration.
- The port security feature does not support the quick EAD deployment feature in 802.1x.

Setting the Maximum Number of MAC Addresses Allowed on a Port

Port security allows more than one user to be authenticated on a port. The number of authenticated users allowed, however, cannot exceed the configured upper limit.

By setting the maximum number of MAC addresses allowed on a port, you can

- Control the maximum number of users who are allowed to access the network through the port
- Control the number of Security MAC addresses that can be added with port security

This configuration is different from that of the maximum number of MAC addresses that can be leaned by a port in MAC address management.

Follow these steps to set the maximum number of MAC addresses allowed on a port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the maximum number of MAC addresses allowed on the port	**port-security max-mac-count** *count-value*	Required Not limited by default

Setting the Port Security Mode

Follow these steps to set the port security mode:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Set the OUI value for user authentication	**port-security oui** *OUI-value* **index** *index-value*	Optional In **userLoginWithOUI** mode, a port supports one 802.1x user plus one user whose source MAC address has a specified OUI value.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the port security mode	**port-security port-mode** { **autolearn** | **mac-and-userlogin-secure** | **mac-and-userlogin-secure-ext** | **mac-authentication** | **mac-else-userlogin-secure** | **mac-else-userlogin-secure-ext** | **secure** | **userlogin** | **userlogin-secure** | **userlogin-secure-ext** | **userlogin-secure-or-mac** | **userlogin-secure-or-mac-ext** | **userlogin-withoui** }	Required By default, a port operates in **noRestriction** mode. In this mode, access to the port is not restricted. You can set a port security mode as needed.

Note

- Before setting the port security mode to **autolearn**, you need to set the maximum number of MAC addresses allowed on the port with the **port-security max-mac-count** command.
- When the port operates in the **autolearn** mode, you cannot change the maximum number of MAC addresses allowed on the port.
- After you set the port security mode to **autolearn**, you cannot configure any static or blackhole MAC addresses on the port.
- If the port is in a security mode other than **noRestriction**, before you can change the port security mode, you need to restore the port security mode to **noRestriction** with the **undo port-security port-mode** command.

If the **port-security port-mode** *mode* command has been executed on a port, none of the following can be configured on the same port:

- Maximum number of MAC addresses that the port can learn
- Reflector port for port mirroring
- Fabric port
- Link aggregation

Configuring Port Security Features

Configuring the NTK feature

Follow these steps to configure the NTK feature:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the NTK feature	**port-security ntk-mode** { **ntkonly** | **ntk-withbroadcasts** | **ntk-withmulticasts** }	Required By default, NTK is disabled on a port, namely all frames are allowed to be sent.

Configuring intrusion protection

Follow these steps to configure the intrusion protection feature:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the corresponding action to be taken by the switch when intrusion protection is triggered	**port-security intrusion-mode** { **blockmac** | **disableport** | **disableport-temporarily** }	Required By default, intrusion protection is disabled.
Return to system view	**quit**	—

To do...	Use the command...	Remarks
Set the timer during which the port remains disabled	**port-security timer disableport** *timer*	Optional 20 seconds by default

Note

The **port-security timer disableport** command is used in conjunction with the **port-security intrusion-mode disableport-temporarily** command to set the length of time during which the port remains disabled.

Caution

If you configure the NTK feature and execute the **port-security intrusion-mode blockmac** command on the same port, the switch will be unable to disable the packets whose destination MAC address is illegal from being sent out that port; that is, the NTK feature configured will not take effect on the packets whose destination MAC address is illegal.

Configuring the Trap feature

Follow these steps to configure port security trapping:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable sending traps for the specified type of event	**port-security trap** { **addresslearned** | **dot1xlogfailure** | **dot1xlogoff** | **dot1xlogon** | **intrusion** | **ralmlogfailure** | **ralmlogoff** | **ralmlogon** }	Required By default, no trap is sent.

Ignoring the Authorization Information from the RADIUS Server

After an 802.1x user or MAC-authenticated user passes Remote Authentication Dial-In User Service (RADIUS) authentication, the RADIUS server delivers the authorization information to the device. You can configure a port to ignore the authorization information from the RADIUS server.

Follow these steps to configure a port to ignore the authorization information from the RADIUS server:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Ignore the authorization information from the RADIUS server	**port-security authorization ignore**	Required By default, a port uses the authorization information from the RADIUS server.

Configuring Security MAC Addresses

Security MAC addresses are special MAC addresses that never age out. One security MAC address can be added to only one port in the same VLAN so that you can bind a MAC address to one port in the same VLAN.

Security MAC addresses can be learned by the auto-learn function of port security or manually configured.

Before adding security MAC addresses to a port, you must configure the port security mode to **autolearn**. After this configuration, the port changes its way of learning MAC addresses as follows.

- The port deletes original dynamic MAC addresses;
- If the amount of security MAC addresses has not yet reach the maximum number, the port will learn new MAC addresses and turn them to security MAC addresses;
- If the amount of security MAC addresses reaches the maximum number, the port will not be able to learn new MAC addresses and the port mode will be changed from **autolearn** to **secure**.

Note

The security MAC addresses manually configured are written to the configuration file; they will not get lost when the port is up or down. As long as the configuration file is saved, the security MAC addresses can be restored after the switch reboots.

Configuration prerequisites

- Port security is enabled.
- The maximum number of security MAC addresses allowed on the port is set.
- The security mode of the port is set to **autolearn**.

Configuring a security MAC address

Follow these steps to configure a security MAC address:

To do...		Use the command...	Remarks
Enter system view		**system-view**	—
Add a security MAC address	In system view	**mac-address security** *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	Either is required. By default, no security MAC address is configured.
	In Ethernet port view	**interface** *interface-type interface-number*	
		mac-address security *mac-address* **vlan** *vlan-id*	

Displaying and Maintaining Port Security Configuration

To do...	Use the command...	Remarks
Display information about port security configuration	**display port-security** [**interface** *interface-list*]	Available in any view
Display information about security MAC address configuration	**display mac-address security** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]	

Port Security Configuration Examples

Port Security Configuration Example

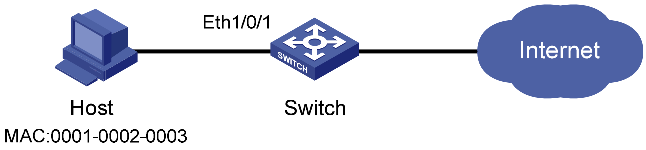
Network requirements

Implement access user restrictions through the following configuration on Ethernet 1/0/1 of the switch.

- Allow a maximum of 80 users to access the port without authentication and permit the port to learn and add the MAC addresses of the users as security MAC addresses.
- To ensure that Host can access the network, add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.
- After the number of security MAC addresses reaches 80, the port stops learning MAC addresses. If any frame with an unknown MAC address arrives, intrusion protection is triggered and the port will be disabled and stay silent for 30 seconds.

Network diagram

Figure 1-1 Network diagram for port security configuration



Configuration procedure

Enter system view.

```
<Switch> system-view
```

Enable port security.

```
[Switch] port-security enable
```

Enter Ethernet1/0/1 port view.

```
[Switch] interface Ethernet 1/0/1
```

Set the maximum number of MAC addresses allowed on the port to 80.

```
[Switch-Ethernet1/0/1] port-security max-mac-count 80
```

Set the port security mode to **autolearn**.

```
[Switch-Ethernet1/0/1] port-security port-mode autolearn
```

Add the MAC address 0001-0002-0003 of Host as a security MAC address to the port in VLAN 1.

```
[Switch-Ethernet1/0/1] mac-address security 0001-0002-0003 vlan 1
```

Configure the port to be silent for 30 seconds after intrusion protection is triggered.

```
[Switch-Ethernet1/0/1] port-security intrusion-mode disableport-temporarily
[Switch-Ethernet1/0/1] quit
[Switch] port-security timer disableport 30
```

Table of Contents

1 DLDP Configuration

When configuring DLDP, go to these sections for information you are interested in:

- Overview
- DLDP Fundamentals
- DLDP Configuration
- DLDP Configuration Example

Overview

Device link detection protocol (DLDP) is an technology for dealing with unidirectional links that may occur in a network.

If two switches, A and B, are connected via a pair of optical fiber cables, one used for sending from A to B, the other sending from B to A, it is a bidirectional link (two-way link). If one of these fibers gets broken, this is a unidirectional link (one-way link).

When a unidirectional link appears, the local device can receive packets from the peer device through the link layer, but the peer device cannot receive packets from the local device. Unidirectional link can cause problems such as network loops.

As for fiber links, two kinds of unidirectional links exist:

- Fiber cross-connection, as shown in Figure 1-1
- Fibers that are not connected or are broken, as shown in Figure 1-2, the hollow lines in which refer to fibers that are not connected or are broken.

Figure 1-1 Fiber cross-connection

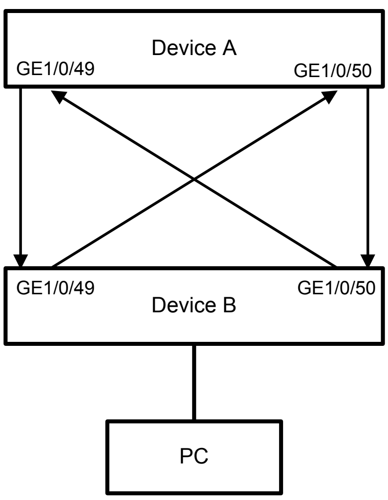
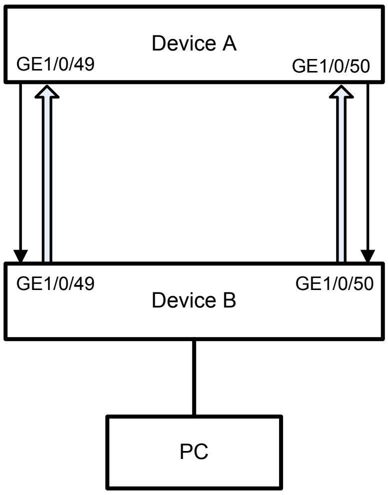


Figure 1-2 Fiber broken or not connected



Device link detection protocol (DLDP) can detect the link status of an optical fiber cable or copper twisted pair (such as super category 5 twisted pair). If DLDP finds a unidirectional link, it disables the related port automatically or prompts you to disable it manually according to the configurations, to avoid network problems.

Note

A copper twisted-pair cable (such as a Category 5e twisted-pair cable) contains eight wires. Some of these wires only transmit data, while the others only receive data. When the wires that only receive data or those that only transmit data all fail while the others are normal, a unidirectional link occurs.

DLDP provides the following features:

- As a link layer protocol, it works together with the physical layer protocols to monitor the link status of a device.
- The auto-negotiation mechanism at the physical layer detects physical signals and faults. DLDP identifies peer devices and unidirectional links, and disables unreachable ports.
- Even if both ends of links can work normally at the physical layer, DLDP can detect whether these links are connected correctly and whether packets can be exchanged normally at both ends. However, the auto-negotiation mechanism cannot implement this detection.

DLDP Fundamentals

DLDP packets

DLDP detects link status by exchanging the following types of packets.

Table 1-1 DLDP packet types

DLDP packet type	Function
Advertisement	Notifies the neighbor devices of the existence of the local device. An advertisement packet carries only the local port information, and it does not require response from the peer end.

DLDP packet type	Function
RSY-Advertisement packets (referred to as RSY packets hereafter)	Advertisement packet with the RSY flag set to 1. RSY advertisement packets are sent to request synchronizing the neighbor information when neighbor information is not locally available or a neighbor information entry ages out.
Flush-Advertisement packets (referred to as flush packets hereafter)	Advertisement packet with the flush flag set to 1. A flush packet carries only the local port information (instead of the neighbor information) and is used to trigger neighbors to remove the information about the local device.
Probe	Probe packets are used to probe the existence of a neighbor. Echo packets are required from the corresponding neighbor. Probe packets carry the local port information. Neighbor information is optional for probe packets. A probe packet carrying neighbor information probes the specified neighbors; A probe packet carrying no neighbor information probes all the neighbors.
Echo	Response to probe packets. An echo packet carries the information about the response port and the neighbor information it maintains. Upon receiving an echo packet, a port checks whether the neighbor information carried in the echo packet is consistent with that of itself. If yes, the link between the local port and the neighbor is regarded as bidirectional.
Disable	Disable packets are used to notify the peer end that the local end is in the disable state. Disable packets carry only the local port information instead of the neighbor information. When a port detects a unidirectional link and enters the disable state, the port sends disable packets to the neighbor. A port enters the disable state upon receiving a disable packet.
LinkDown	Linkdown packets are used to notify unidirectional link emergencies (a unidirectional link emergency occurs when the local port is down and the peer port is up). Linkdown packets carry only the local port information instead of the neighbor information. In some conditions, a port is considered to be physically down if the link connecting to the port is physically abnormal (for example, the Rx line of the fiber on the port is disconnected, while the Tx line operates properly). But for the peer end, as Rx signals can still be received on the physical layer, the port is still considered to be normal. Such a situation is known as unidirectional link emergency. When a unidirectional link emergency occurs, DLDP sends linkdown packets immediately to inform the peer of the link abnormality. Without linkdown packets, the peer can detect the link abnormality only after a period when the corresponding neighbor information maintained on the neighbor device ages out, which is three times the advertisement interval. Upon receiving a linkdown packet, if the peer end operates in the enhanced mode, it enters the disable state, and sets the receiving port to the DLDP down state (auto shutdown mode) or gives an alarm to the user (manual shutdown mode).
Recover Probe	Recover probe packets are used to detect whether a link recovers to implement the port auto-recovery mechanism. Recover probe packets carry only the local port information instead of the neighbor information. They request for recover echo packets as the response. A port in the DLDP down state sends a recover probe packet every two seconds.
Recover Echo	Recover echo packets are response to recover probe packets in the port auto-recovery mechanism. A link is considered to restore to the bidirectional state if a port on one end sends a recover probe packet, receives a recover echo packet, and the neighbor information contained in the recover echo packet is consistent with that of the local port.

DLDP Status

A link can be in one of these DLDP states: initial, inactive, active, advertisement, probe, disable, and delaydown.

Table 1-2 DLDP status

Status	Description
Initial	Initial status before DLDP is enabled.
Inactive	DLDP is enabled but the corresponding link is down
Active	DLDP is enabled, and the link is up or an neighbor entry is cleared
Advertisement	All neighbors communicate normally in both directions, or DLDP remains in active state for more than five seconds and enters this status. It is a stable state where no unidirectional link is found
Probe	DHCP sends packets to check whether the link is a unidirectional. It enables the probe sending timer and an echo waiting timer for each target neighbor.
Disable	DLDP detects a unidirectional link, or finds (in enhanced mode) that a neighbor disappears. In this case, DLDP sends and receives only recover probe packets and recover echo packets.
DelayDown	When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first. When a device changes to the delaydown state, the related DLDP neighbor information remains, and the DelayDown timer is triggered. After the DelayDown timer expires, the DLDP neighbor information is removed.

DLDP Timers

Table 1-3 DLDP timers

Timer	Description
Advertisement sending timer	Interval between sending advertisement packets, which can be configured on a command line interface. By default, the timer length is 5 seconds.
Probe sending timer	The interval is 0.5 seconds. In the probe state, DLDP sends two probe packets in a second.
Echo waiting timer	It is enabled when DLDP enters the probe state. The echo waiting timer length is 10 seconds. If no echo packet is received from the neighbor when the Echo waiting timer expires, the state of the local end is set to unidirectional link (one-way audio) and the state machine turns into the **disable** state. DLDP outputs log and tracking information, sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. At the same time, DLDP deletes the neighbor entry.

Timer	Description
Entry aging timer	When a new neighbor joins, a neighbor entry is created and the corresponding entry aging timer is enabled When an advertisement packet is received from a neighbor, the neighbor entry is updated and the corresponding entry aging timer is updated In the normal mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP sends an advertisement packet with an RSY tag, and deletes the neighbor entry. In the enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer The entry aging timer length is three times the advertisement timer length.
Enhanced timer	In the enhanced mode, if no packet is received from the neighbor when the entry aging timer expires, DLDP enables the enhanced timer for the neighbor. The enhanced timer length is 10 seconds The enhanced timer then sends one probe packet every second and eight packets successively to the neighbor. If no echo packet is received from the neighbor when the enhanced timer expires, the state of the local end is set to unidirectional communication state and the state machine turns into the **disable** state. DLDP outputs log and tracking information and sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. Meanwhile, DLDP deletes the neighbor entry.
DelayDown timer	When a device in the active, advertisement, or probe DLDP state receives a port down message, it does not removes the corresponding neighbor immediately, neither does it changes to the inactive state. Instead, it changes to the delaydown state first. When a device changes to the delaydown state, the related DLDP neighbor information remains, and the DelayDown timer is triggered. The DelayDown timer is configurable and ranges from 1 to 5 seconds. A device in the delaydown state only responds to port up messages. A device in the delaydown state resumes its original DLDP state if it receives a port up message before the delaydown timer expires. Otherwise, it removes the DLDP neighbor information and changes to the inactive state.

DLDP Operating Mode

DLDP can operate in two modes: normal mode and enhanced mode, as described below.

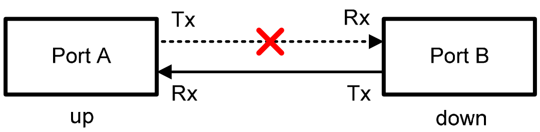
- In normal DLDP mode, when an entry timer expires, the device removes the corresponding neighbor entry and sends an Advertisement packet with RSY tag.
- In enhanced DLDP mode, when an entry timer expires, the Enhanced timer is triggered and the device sends up to eight Probe packets at a frequency of one packet per second to test the neighbor. If no Echo packet is received from the neighbor when the Echo timer expires, the device transits to the Disable state.

Table 1-4 DLDP operating mode and neighbor entry aging

DLDP operating mode	Detecting a neighbor after the corresponding neighbor entry ages out	Removing the neighbor entry immediately after the Entry timer expires	Triggering the Enhanced timer after an Entry timer expires
Normal mode	No	Yes	No
Enhanced mode	Yes	No	Yes (When the enhanced timer expires, the state of the local end is set to unidirectional link, and the neighbor entry is aged out.)

The enhanced DLDP mode is designed for addressing black holes. It prevents the cases where one end of a link is up and the other is down. If you configure the speed and the duplex mode by force on a device, the situation shown in Figure 1-3 may occur, where Port B is actually down but the state of Port B cannot be detected by common data link protocols, so Port A is still up. In enhanced DLDP mode, however, Port A tests Port B after the Entry timer concerning Port B expires. Port A then transits to the Disable state if it receives no Echo packet from Port A when the Echo timer expires. As Port B is physically down, it is in the Inactive DLDP state.

Figure 1-3 A case for Enhanced DLDP mode



Note

- In normal DLDP mode, only fiber cross-connected unidirectional links (as shown in Figure 1-1) can be detected.
- In enhanced DLDP mode, two types of unidirectional links can be detected. One is fiber cross-connected links (as shown in Figure 1-1). The other refers to fiber pairs with one fiber not connected or disconnected (as shown in Figure 1-2). To detect unidirectional links that are of the latter type, you need to configure the ports to operate at specific speed and in full duplex mode. Otherwise, DLDP cannot take effect.

DLDP Implementation

1) If the DLDP-enabled link is up, DLDP sends DLDP packets to the peer device, and analyzes/processes the DLDP packets received from the peer device. DLDP packets sent in different DLDP states are of different types.

Table 1-5 DLDP state and DLDP packet type

DLDP state	Type of the DLDP packets sent
Active	Advertisement packets, with the RSY flag set or not set.
Advertisement	Advertisement packets
Probe	Probe packets

2) A DLDP packet received is processed as follows:

- In authentication mode, the DLDP packet is authenticated and is then dropped if it fails the authentication.
- The packet is further processed, as described in Table 1-6.

Note

You can prevent network attacks and illegal detect through DLDP authentication. Three DLDP authentication modes exist: non-authentication, plain text authentication, MD5 authentication.

Table 1-6 The procedure to process a received DLDP packet

<table>
<tr><th>Packet type</th><th colspan="5">Processing procedure</th></tr>
<tr><td rowspan="2">Advertisement packet</td><td colspan="2" rowspan="2">Extracts neighbor information</td><td colspan="3">If the corresponding neighbor entry does not exist on the local device, DLDP creates the neighbor entry, triggers the entry aging timer, and switches to the probe state.</td></tr>
<tr><td colspan="3">If the corresponding neighbor entry already exists on the local device, DLDP resets the aging timer of the entry.</td></tr>
<tr><td>Flush packet</td><td colspan="5">Removes the neighbor entry from the local device</td></tr>
<tr><td rowspan="2">Probe packet</td><td colspan="2" rowspan="2">Sends echo packets containing both neighbor and its own information to the peer</td><td colspan="3">Creates the neighbor entry if it does not exist on the local device.</td></tr>
<tr><td colspan="3">Resets the aging timer of the entry if the neighbor entry already exists on the local device.</td></tr>
<tr><td rowspan="4">Echo packet</td><td rowspan="4">Checks to see if the local device is in the probe state</td><td>No</td><td colspan="3">Drops the echo packet</td></tr>
<tr><td rowspan="3">Yes</td><td rowspan="3">Checks to see if the neighbor information contained in the packet is the same as that on the local device</td><td>No</td><td>Drops the echo packet</td></tr>
<tr><td rowspan="2">Yes</td><td>Sets the flag bit of the neighbor to bidirectional link</td></tr>
<tr><td>If all neighbors are in the bidirectional link state, DLDP switches from the probe state to the advertisement state, and sets the echo waiting timer to 0.</td></tr>
</table>

3) If no echo packet is received from the neighbor, DLDP performs the following processing:

Table 1-7 Processing procedure when no echo packet is received from the neighbor

No echo packet received from the neighbor	Processing procedure
In normal mode, no echo packet is received when the echo waiting timer expires.	DLDP switches to the **disable** state, outputs log and tracking information, and sends flush packets. Depending on the user-defined DLDP down mode, DLDP disables the local port automatically or prompts you to disable the port manually. DLDP sends RSY messages and removes the corresponding neighbor entries.
In enhanced mode, no echo packet is received when the enhanced timer expires	

DLDP Neighbor State

A DLDP neighbor can be in one of these two states: two way and unknown. You can check the state of a DLDP neighbor by using the **display dldp** command.

Table 1-8 Description on the two DLDP neighbor states

DLDP neighbor state	Description
two way	The link to the neighbor operates properly.
unknown	The device is detecting the neighbor and the neighbor state is unknown.

Link Auto-recovery Mechanism

If the shutdown mode of a port is set to auto shutdown, the port is set to the DLDP down state when DLDP detects the link connecting to the port is a unidirectional link. A port in DLDP down state does not forward service packets or receive/send protocol packets except DLDPDUs.

A port in the DLDP down state recovers when the corresponding link recovers. A port in the DLDP down state sends recover probe packets periodically. On receiving a correct recover echo packet (which means that the unidirectional link is restored to a bidirectional link), it is brought up by DLDP. The detailed process is as follows.

1) A port in the DLDP down state sends a recover probe packet every 2 seconds. Recover probe packets carry only the local port information.
2) Upon receiving a recover probe packet, the peer end responds with a recover echo packet.
3) Upon receiving a recover echo packet, the local end checks to see if the neighbor information carried in the recover echo packet is consistent with that of the local port. If yes, the link between the local port and the neighbor is considered to be recovered to bidirectional, the port changes from the disable state to the active state, and neighboring relationship is reestablished between the local port and the neighbor.

Note

Only ports in the DLDP down state can send and process recover probe packets and recover echo packets. The auto-recovery mechanism does apply to ports that are shut down manually.

DLDP Configuration

Performing Basic DLDP Configuration

Follow these steps to perform basic DLDP configuration:

<table>
<tr><th colspan="3">To do …</th><th>Use the command …</th><th>Remarks</th></tr>
<tr><td colspan="3">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td rowspan="3">Enable DLDP</td><td colspan="2">Enable DLDP on all optical ports of the switch</td><td>dldp enable</td><td rowspan="3">Required.
By default, DLDP is disabled.</td></tr>
<tr><td rowspan="2">Enable DLDP on the current port (a non-optical port or an optical port)</td><td>Enter Ethernet port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>Enable DLDP</td><td>dldp enable</td></tr>
<tr><td colspan="3">Set the authentication mode and password</td><td>dldp authentication-mode { none | simple simple-password | md5 md5-password }</td><td>Optional.
By default, the authentication mode is none.</td></tr>
<tr><td colspan="3">Set the interval of sending DLDP packets</td><td>dldp interval timer-value</td><td>Optional.
By default, the interval is 5 seconds.</td></tr>
<tr><td colspan="3">Set the delaydown timer</td><td>dldp delaydown-timer delaydown-time</td><td>Optional
By default, the delaydown timer expires after 1 second it is triggered.</td></tr>
<tr><td colspan="3">Set the DLDP handling mode when an unidirectional link is detected</td><td>dldp unidirectional-shutdown { auto | manual }</td><td>Optional.
By default, the handling mode is auto.</td></tr>
<tr><td colspan="3">Set the DLDP operating mode</td><td>dldp work-mode { enhance | normal }</td><td>Optional.
By default, DLDP works in normal mode.</td></tr>
</table>

Note the following when performing basic DLDP configuration.

- DLDP can detect unidirectional links only after the links are connected. Therefore, before enabling DLDP, make sure that optical fibers or copper twisted pairs are connected.
- To ensure unidirectional links can be detected, make sure DLDP is enabled on both sides; and the interval for sending advertisement packets, authentication mode, and password are the same on both sides.
- The interval for sending advertisement packets ranges from 1 to 100 seconds and defaults to 5 seconds. You can adjust this setting as needed to enable DLDP to respond in time to link failures. If the interval is too long, STP loops may occur before unidirectional links are terminated; if the interval is too short, network traffic may increase in vain and available bandwidth decreases. Normally, the interval is shorter than one-third of the STP convergence time, which is generally 30 seconds.
- DLDP does not process any link aggregation control protocol (LACP) event, and treats each link in the aggregation group as independent.

- When connecting two DLDP-enabled devices, make sure the software running on them is of the same version. Otherwise, DLDP may operate improperly.
- When you use the **dldp enable/dldp disable** command in system view to enable/disable DLDP on all optical ports of the switch, the configuration takes effect on the existing optical ports, instead of those added subsequently.
- Make sure the authentication mode and password configured on both sides are the same for DLDP to operate properly.
- When DLDP works in enhanced mode, the system can identify two types of unidirectional links: one is caused by fiber cross-connection and the other is caused by one fiber being not connected or being disconnected.
- When DLDP works in normal mode, the system can identify unidirectional links caused by fiber cross-connection.
- When the device is busy with services and the CPU utilization is high, DLDP may issue mistaken reports. You are recommended to configure the operating mode of DLDP as manual after unidirectional links are detected, so as to reduce the influence of mistaken reports.

Resetting DLDP State

You can reset the DLDP state for the ports shut down by DLDP due to unidirectional links to enable DLDP detection again.

Note

This function is only applicable to ports that are in DLDP down state.

Follow these steps to reset DLDP state:

To do …	Use the command …	Remarks
Reset DLDP state for all the ports shut down by DLDP	**system-view**	Select either of the two.
	dldp reset	
Reset the DLDP state for a port shut down by DLDP	**interface** *interface-type interface-number*	
	dldp reset	

Displaying and Maintaining DLDP

To do …	Use the command …	Remarks
Display the DLDP configuration of a unit or a port	**display dldp** { *unit-id* | *interface-type interface-number* }	Available in any view.

DLDP Configuration Example

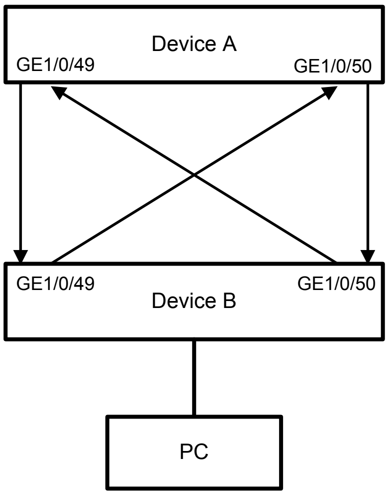
Network requirements

As shown in Figure 1-4,

- Switch A and Switch B are connected through two pairs of fibers. Both of them support DLDP. All the ports involved operate in mandatory full duplex mode, with their rates all being 1,000 Mbps.
- Suppose the fibers between Switch A and Switch B are cross-connected. DLDP disconnects the unidirectional links after detecting them.
- After the fibers are connected correctly, the ports shut down by DLDP are restored.

Network diagram

Figure 1-4 Network diagram for DLDP configuration



Configuration procedure

1) Configure Switch A

Configure the ports to work in mandatory full duplex mode at a rate of 1000 Mbps.

```
<SwitchA> system-view
[SwitchA] interface gigabitethernet 1/0/49
[SwitchA-GigabitEthernet1/0/49] duplex full
[SwitchA-GigabitEthernet1/0/49] speed 1000
[SwitchA-GigabitEthernet1/0/49] quit
[SwitchA] interface gigabitethernet 1/0/50
[SwitchA-GigabitEthernet1/0/50] duplex full
[SwitchA-GigabitEthernet1/0/50] speed 1000
[SwitchA-GigabitEthernet1/0/50] quit
```

Enable DLDP globally

```
[SwitchA] dldp enable
```

Set the interval between sending DLDP packets to 15 seconds.

```
[SwitchA] dldp interval 15
```

Configure DLDP to work in enhanced mode

```
[SwitchA] dldp work-mode enhance
```

Set the DLDP handling mode for unidirectional links to **auto**.

```
[SwitchA] dldp unidirectional-shutdown auto
```

Display the DLDP state

```
[SwitchA] display dldp 1
```

Note

When two switches are connected through fibers in a crossed way, two or three ports may be in the disable state, and the rest in the inactive state.

When a fiber is connected to a device correctly on one end with the other end connected to no device:

- If the device operates in the normal DLDP mode, the end that receives optical signals is in the advertisement state; the other end is in the inactive state.
- If the device operates in the enhance DLDP mode, the end that receives optical signals is in the disable state; the other end is in the inactive state.

Restore the ports shut down by DLDP

```
[SwitchA] dldp reset
```

2) Configure Switch B

The configuration of Switch B is the same to that of Switch A and is thus omitted.

Table of Contents

1 MAC Address Table Management

When MAC address table management functions, go to these sections for information you are interested in:

- Overview
- MAC Address Table Management
- Displaying MAC Address Table Information
- Configuration Example

Note

This chapter describes the management of static, dynamic, and blackhole MAC address entries. For information about the management of multicast MAC address entries, refer to *Multicast Operation*.

Overview

Introduction to the MAC Address Table

An Ethernet switch is mainly used to forward packets at the data link layer, that is, transmit the packets to the corresponding ports according to the destination MAC address of the packets. To forward packets quickly, a switch maintains a MAC address table, which is a Layer 2 address table recording the MAC address-to-forwarding port association. Each entry in a MAC address table contains the following fields:

- Destination MAC address
- ID of the VLAN which a port belongs to
- Forwarding egress port number on the local switch

When forwarding a packet, an Ethernet switch adopts one of the two forwarding methods based upon the MAC address table entries.

- Unicast forwarding: If the destination MAC address carried in the packet is included in a MAC address table entry, the switch forwards the packet through the forwarding egress port in the entry.
- Broadcast forwarding: If the destination MAC address carried in the packet is not included in the MAC address table, the switch broadcasts the packet to all ports except the one that originally received the packet.

Introduction to MAC Address Learning

MAC address table entries can be updated and maintained through the following two ways:

- Manual configuration
- MAC address learning

Generally, the majority of MAC address entries are created and maintained through MAC address learning. The following describes the MAC address learning process of a switch:

1) As shown in Figure 1-1, User A and User B are both in VLAN 1. When User A communicates with User B, the packet from User A comes into the switch on GigabitEthernet 1/0/1. At this time, the switch records the source MAC address of the packet, that is, the address MAC-A of User A to the MAC address table of the switch, forming an entry shown in Figure 1-2.

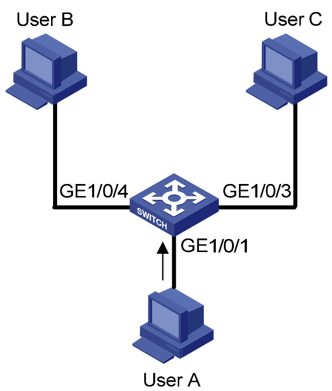


Figure 1-1 MAC address learning diagram (1)

MAC-address	Port	VLAN ID
MAC-A	GigabitEthernet1/0/1	1

Figure 1-2 MAC address table entry of the switch (1)

2) After learning the MAC address of User A, the switch starts to forward the packet. Because there is no MAC address and port information of User B in the existing MAC address table, the switch forwards the packet to all ports except GigabitEthernet 1/0/1 to ensure that User B can receive the packet.

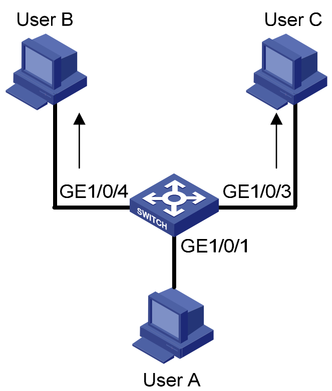


Figure 1-3 MAC address learning diagram (2)

3) Because the switch broadcasts the packet, both User B and User C can receive the packet. However, User C is not the destination device of the packet, and therefore does not process the packet. Normally, User B will respond to User A, as shown in Figure 1-4. When the response packet from User B comes into the switch on GigabitEthernet 1/0/4, the switch records the association between the MAC address of User B and the corresponding port to the MAC address table of the switch.

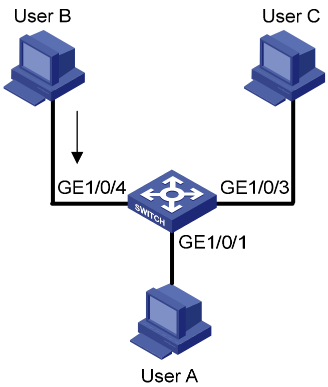


Figure 1-4 MAC address learning diagram (3)

4) At this time, the MAC address table of the switch includes two forwarding entries shown in Figure 1-5. When forwarding the response packet from User B to User A, the switch sends the response to User A through GigabitEthernet 1/0/1 (technically called unicast), because MAC-A is already in the MAC address table.

MAC-address	Port	VLAN ID
MAC-A	GigabitEthernet1/0/1	1
MAC-B	GigabitEthernet1/0/4	1

Figure 1-5 MAC address table entries of the switch (2)

5) After this interaction, the switch sends packets destined for User A and User B in unicast mode based on the corresponding MAC address table entries.

Note

- Under some special circumstances, for example, User B is unreachable or User B receives the packet but does not respond to it, the switch cannot learn the MAC address of User B. Hence, the switch still broadcasts the packets destined for User B.
- The switch learns only unicast addresses by using the MAC address learning mechanism but directly drops any packet with a broadcast source MAC address.

Managing MAC Address Table

Aging of MAC address table

To fully utilize a MAC address table, which has a limited capacity, the switch uses an aging mechanism for updating the table. That is, the switch starts an aging timer for an entry when dynamically creating the entry. The switch removes the MAC address entry if no more packets with the MAC address recorded in the entry are received within the aging time.

Note

- The MAC address aging timer only takes effect on dynamic MAC address entries.
- With the "destination MAC address triggered update function" enabled, when a switch finds a packet with a destination address matching one MAC address entry within the aging time, it updates the entry and restarts the aging timer.

Entries in a MAC address table

Entries in a MAC address table fall into the following categories according to their characteristics and configuration methods:

- Static MAC address entry: Also known as permanent MAC address entry. This type of MAC address entries are added/removed manually by the network operator and cannot age out by themselves. Using static MAC address entries can greatly reduce broadcast packets and are suitable for networks where network devices seldom change.
- Dynamic MAC address entry: This type of MAC address entries age out after the configured aging time. They are generated by the MAC address learning mechanism or configured manually.
- Blackhole MAC address entry: This type of MAC address entries are configured manually. A switch discards the packets destined for or originated from the MAC addresses contained in blackhole MAC address entries. Blackhole entries are configured for filtering out frames with specific source or destination MAC addresses.

Table 1-1 lists the different types of MAC address entries and their characteristics.

Table 1-1 Characteristics of different types of MAC address entries

MAC address entry	Configuration method	Aging time	Preserved or not at reboot (if the configuration is saved)
Static MAC address entry	Manually configured	Unavailable	Yes
Dynamic MAC address entry	Manually configured or generated by MAC address learning mechanism	Available	No
Blackhole MAC address entry	Manually configured	Unavailable	Yes

MAC Address Table Management

MAC Address Table Management Configuration Task List

Complete the following tasks to configure MAC address table management:

Task	Remarks
Configuring a MAC Address Entry	Required
Setting the MAC Address Aging Timer	Optional
Setting the Maximum Number of MAC Addresses a Port Can Learn	Optional

Task	Remarks
Enabling Destination MAC Address Triggered Update	Optional

Configuring a MAC Address Entry

You can add, modify, or remove a MAC address entry, remove all MAC address entries concerning a specific port, or remove specific type of MAC address entries (dynamic or static MAC address entries).

Adding a MAC address entry in system view

You can add a MAC address entry in either system view or Ethernet port view.

Follow these steps to add a MAC address entry in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Add a MAC address entry	**mac-address** { **static** | **dynamic** | **blackhole** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*	Required

Caution

- When you add a MAC address entry, the port specified by the **interface** argument must belong to the VLAN specified by the **vlan** argument in the command. Otherwise, you will fail to add this MAC address entry.,By default, all ports belong to VLAN 1.
- If the VLAN specified by the **vlan** argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

Adding a MAC address entry in Ethernet port view

Follow these steps to add a MAC address entry in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add a MAC address entry	**mac-address** { **static** | **dynamic** | **blackhole** } *mac-address* **vlan** *vlan-id*	Required

Caution

- When you add a MAC address entry, the current port must belong to the VLAN specified by the **vlan** argument in the command. Otherwise, the entry will not be added.
- If the VLAN specified by the **vlan** argument is a dynamic VLAN, after a static MAC address is added, it will become a static VLAN.

Setting the MAC Address Aging Timer

Setting an appropriate MAC address aging timer is important for the switch to run efficiently.

- If the aging timer is set too long, excessive invalid MAC address entries maintained by the switch may fill up the MAC address table. This prevents the MAC address table from being updated with network changes in time.
- If the aging timer is set too short, the switch may remove valid MAC address entries. This decreases the forwarding performance of the switch.

Follow these steps to set aging time of MAC address entries:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the MAC address aging timer	**mac-address timer** { **aging** *age* | **no-aging** }	Required The default is 300 seconds.

The capacity of the MAC address table on a switch is limited. After the limit is reached, the switch will forward the frames received with unknown source MAC addresses without learning MAC addresses. In case the MAC address table gets full, you can tune the aging timer to a smaller value to speed up MAC address entry aging so that new MAC addresses can be learned

Normally, you are recommended to use the default aging timer, namely, 300 seconds.

The **no-aging** keyword specifies that MAC address entries never age out.

Note

MAC address aging configuration applies to all ports, but only takes effect on dynamic MAC addresses, which are either learnt or configured.

Setting the Maximum Number of MAC Addresses a Port Can Learn

The MAC address learning mechanism enables an Ethernet switch to acquire the MAC addresses of the network devices on the segment connected to the ports of the switch. By searching the MAC address table, the switch directly forwards the packets destined for these MAC addresses through the hardware, improving the forwarding efficiency. A MAC address table too big in size may prolong the time for searching MAC address entries, thus decreasing the forwarding performance of the switch.

By setting the maximum number of MAC addresses that can be learned from individual ports, the administrator can control the number of the MAC address entries the MAC address table can dynamically maintain. When the number of the MAC address entries learnt from a port reaches the set value, the port stops learning MAC addresses.

Follow these steps to set the maximum number of MAC addresses a port can learn:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the maximum number of MAC addresses the port can learn	**mac-address max-mac-count** *count*	Required By default, the number of the MAC addresses a port can learn is not limited.

Note

If you have configured the maximum number of MAC addresses that a port can learn, you cannot enable the MAC address authentication or port security functions on the port, and vice versa.

Enabling Destination MAC Address Triggered Update

By default, a switch updates its MAC address entries based on the source MAC addresses of packets. However, this may cause the switch to perform unnecessary broadcasts in some applications. For example, when a port aggregation group is used in a stacked configuration (IRF) for communications, MAC address entries of some ports in the aggregation group may not be updated in time, resulting in unnecessary broadcasts.

The destination MAC address triggered update function solves the above problem by allowing the switch to update its MAC address entries according to destination MAC addresses in addition to source MAC addresses. This function improves the availability of the MAC address table.

Follow these steps to enable destination MAC address triggered update:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable destination MAC address triggered update	**mac-address aging destination-hit enable**	Required Disabled by default

Displaying MAC Address Table Information

To do…	Use the command…	Remarks
Display information about the MAC address table	**display mac-address** [*display-option*]	Available in any view

To do…	Use the command…	Remarks
Display the aging time of the dynamic MAC address entries in the MAC address table	**display mac-address aging-time**	
Display the configured start port MAC address	**display port-mac**	

Configuration Examples

Adding a Static MAC Address Entry Manually

Network requirements

The server connects to the switch through GigabitEthernet 1/0/2. To prevent the switch from broadcasting packets destined for the server, it is required to add the MAC address of the server to the MAC address table of the switch, which then forwards packets destined for the server through GigabitEthernet 1/0/2.

- The MAC address of the server is 000f-e20f-dc71.
- Port GigabitEthernet 1/0/2 belongs to VLAN 1.
- Suppose the MAC address of a host is 000f-e235-abcd and belongs to VLAN 1. Because the host once behaved suspiciously on the network, you can add a blackhole MAC address entry for the MAC address to drop all packets destined for the host for security sake.

Configuration procedure

Enter system view.

```
<Sysname> system-view
[Sysname]
```

Add a MAC address, with the VLAN, ports, and states specified.

```
[Sysname] mac-address static 000f-e20f-dc71 interface GigabitEthernet 1/0/2 vlan 1
```

Add a black hole MAC address 000f-e235-abcd, with the VLAN and ports specified.

```
[Sysname] mac-address blackhole 000f-e235-abcd interface GigabitEthernet 1/0/2 vlan 1
```

Display information about the current MAC address table.

```
[Sysname] display mac-address interface GigabitEthernet 1/0/2
Unit 1
MAC ADDR          VLAN ID  STATE         PORT INDEX            AGING TIME(s)
000f-e20f-dc71    1        Config static GigabitEthernet1/0/2 NOAGED
000f-e235-abcd    1        Blackhole     GigabitEthernet1/0/2 NOAGED
000f-e20f-a7d6    1        Learned       GigabitEthernet1/0/2 AGING
000f-e20f-b1fb    1        Learned       GigabitEthernet1/0/2 AGING
000f-e20f-f116    1        Learned       GigabitEthernet1/0/2 AGING
---  4 mac address(es) found on port GigabitEthernet1/0/2 ---
```

Table of Contents

1 Auto Detect Configuration

When configuring the auto detect function, go to these sections for information you are interested in:

- Introduction to the Auto Detect Function
- Auto Detect Configuration
- Auto Detect Configuration Examples

Introduction to the Auto Detect Function

The Auto Detect function uses Internet Control Message Protocol (ICMP) request/reply packets to test network connectivity regularly between the Auto Detect-enabled switch and the detected object.

The detected object of the Auto Detect function is a detected group, which is a set of IP addresses. To check the reachability to a detected group, a switch enabled with Auto Detect sends ICMP requests to the IP addresses in the group and waits for the ICMP replies from the group based on the user-defined policy (which includes the number of ICMP requests and the timeout waiting for a reply). Then according to the check result, the switch determines whether to make the applications using the detected group take effect.

Currently, the following features are used in conjunction with Auto Detect:

- Static route
- Interface backup

Note

- When the Auto Detect feature is used in conjunction with multiple features (static routing, or interface backup), if the detected object is the same, you can apply a detected group to multiple features, thus reducing the configuration workload.
- For details about static routing, refer to the Routing Protocol part of the manual.

Auto Detect Configuration

Complete the following tasks to configure auto detect:

Task	Remarks
Auto Detect Basic Configuration	Required
Auto Detect Implementation in Static Routing	Optional

Task	Remarks
Auto Detect Implementation in VLAN Interface Backup	Optional

Auto Detect Basic Configuration

Follow these steps to configure the auto detect function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a detected group and enter detected group view	**detect-group** *group-number*	Required
Add an IP address to be detected to the detected group	**detect-list** *list-number* **ip address** *ip-address* [**nexthop** *ip-address*]	Required
Specify a relationship between detected IP addresses in the group	**option** [**and** | **or**]	Optional By default, the **and** keyword is specified.
Set an interval between detecting operations	**timer loop** *interval*	Optional By default, the detecting interval is 15 seconds.
Set the number of ICMP requests during a detecting operation	**retry** *retry-times*	Optional By default, the number is 2.
Set a timeout waiting for an ICMP reply	**timer wait** *seconds*	Optional By default, the timeout is 2 seconds.
Display the detected group configuration	**display detect-group** [*group-number*]	Available in any view

Note

If the relationship between IP addresses of a detected group is **and**, any unreachable IP address in the group makes the detected group unreachable and the remaining IP addresses will not be detected. If the relationship is **or**, any reachable IP address makes the detected group reachable and the remaining IP addresses will not be detected.

Auto Detect Implementation in Static Routing

A static route is a special route. It is manually configured by the administrator. With a static route configured, the data packets to the specified destination will be forwarded along the path specified by the administrator.

The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topology change occurs to the network, the routes may be unreachable and the network may break.

To avoid such problems, you can configure another route to back up the static route and use the Auto Detect function to judge the validity of the static route. If the static route is valid, packets are forwarded according to the static route, and the other route is standby. If the static route is invalid, packets are forwarded according to the backup route. In this way, the communication is not interrupted, and the network reliability is improved.

You can bind the static route with a detected group. The Auto Detect function will then detect the group and judge the validity of the static route according to the returned reachable/unreachable information..

- The static route is valid if the detected group is **reachable**.
- The static route is invalid if the detected group is **unreachable**.

Note

You need to create the detected group before performing the following operations.

Follow these steps to configure the auto detect function for a static route:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Bind a detected group to a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**] **detect-group** *group-number*	Required

Auto Detect Implementation in VLAN Interface Backup

VLAN interface backup means backing up the VLAN interfaces on a devices. Usually, the master VLAN interface transmits traffic, while the backup VLAN interfaces stay standby. When the master VLAN interface or the link connected to the VLAN interface fails and thus cannot transmit traffic, the backup VLAN interface can be used for communication. In this way, the network reliability is improved.

As shown in Figure 1-1, Switch A has two VLAN interfaces: VLAN-interface 1 and VLAN-interface 2. The two VLAN-interfaces back up each other. Normally. VLAN-interface 1 transmits traffic, while VLAN-interface 2 stays standby. When VLAN-interface 1 or the link connected to VLAN-interface 1 fails and thus cannot transmit traffic normally, VLAN-interface 2 takes over to transmit traffic. In this way, the traffic can be transmitted smoothly without interruption.

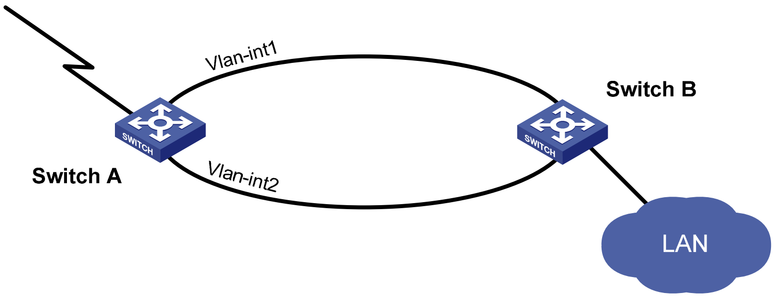


Figure 1-1 Schematic diagram for VLAN interface backup

Using Auto Detect can help implement VLAN interfaces backup. When data can be transmitted through two VLAN interfaces on the switch to the same destination, configure one of the VLAN interface as the active interface and the other as the standby interface. The standby interface is enabled automatically when the active fails, so as to ensure the data transmission. In this case, the Auto Detect function is implemented as follows:

- In normal situations (that is, when the detected group is **reachable**), the standby VLAN interface is down and packets are transmitted through the active VLAN interface.
- When the link between the active VLAN interface and the destination faults (that is, the detected group is **unreachable**), the system enables the backup VLAN interface.
- When the link between the active VLAN interface and the destination recovers (that is, the detected group becomes **reachable** again), the system shuts down the standby VLAN interface again.

Note

You need to create the detected group and perform configurations concerning VLAN interfaces before the following operations.

Follow these steps to configure the auto detect function for VLAN interface backup:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Enable the auto detect function to implement VLAN interface backup	**standby detect-group** *group-number*	Required This operation is only needed on the secondary VLAN interface.

Auto Detect Configuration Examples

Configuration Example for Auto Detect Implementation with Static Routing

Network requirements

- Create detected group 8 on Switch A; detect the reachability of the IP address 10.1.1.4, with 192.168.1.2 as the next hop, and the detecting number set to 1.

- On switch A, configure a static route to Switch C.
- Enable the static route when the detected group 8 is **reachable**.
- To ensure normal operating of the auto detect function, configure a static route to Switch A on Switch C.

Network diagram

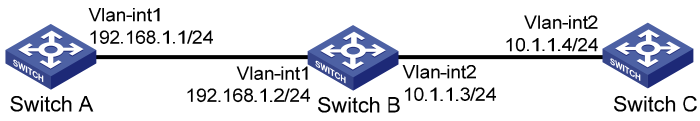


Figure 1-2 Network diagram for implementing the auto detect function in static route

Configuration procedure

Configure the IP addresses of all the interfaces as shown in Figure 1-2. The configuration procedure is omitted.

- Configure Switch A.

Enter system view.

```
<SwitchA> system-view
```

Create detected group 8.

```
[SwitchA] detect-group 8
```

Detect the reachability of 10.1.1.4/24, with 192.168.1.2/24 as the next hop, and the detecting number set to 1.

```
[SwitchA-detect-group-8] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
[SwitchA-detect-group-8] quit
```

Enable the static route when the detected group is reachable. The static route is invalid when the detected group is unreachable.

```
[SwitchA] ip route-static 10.1.1.4 24 192.168.1.2 detect-group 8
```

- Configure Switch C.

Enter system view.

```
<SwitchC> system-view
```

Configure a static route to Switch A.

```
[SwitchC] ip route-static 192.168.1.1 24 10.1.1.3
```

Configuration Example for Auto Detect Implementation with VLAN Interface Backup

Network requirements

- Make sure the routes between Switch A, Switch B, and Switch C, and between Switch A, Switch D, and Switch C are reachable.
- Create detected group 10 on Switch A to detect the connectivity between Switch B and Switch C.
- Configure VLAN-interface 1 to be the active interface, which is enabled when the detected group 10 is **reachable**.
- Configure VLAN-interface 2 to be the standby interface, which is enabled when the detected group 10 is **unreachable**.

Network diagram

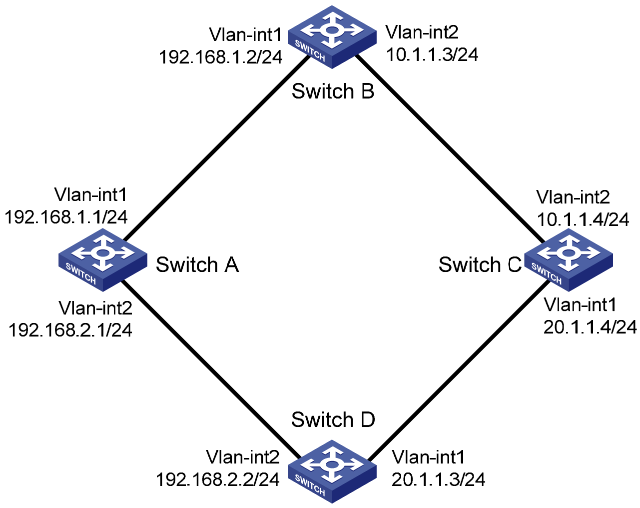


Figure 1-3 Network diagram for VLAN interface backup

Configuration procedure

Configure the IP addresses of all the interfaces as shown in Figure 1-3. The configuration procedure is omitted.

Enter system view.

```
<SwitchA> system-view
```

Create auto detected group 10.

```
[SwitchA] detect-group 10
```

Add the IP address of 10.1.1.4 to detected group 10 to detect the reachability of the IP address, with the IP address of 192.168.1.2 as the next hop, and the detecting number set to 1.

```
[SwitchA-detect-group-10] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
[SwitchA-detect-group-10] quit
```

Specify to enable VLAN-interface 2 when the result of detected group 10 is **unreachable**.

```
[SwitchA] interface vlan-interface 2
[SwitchA-Vlan-interface2] standby detect-group 10
```

Table of Contents

1 MSTP Configuration

Go to these sections for information you are interested in:

Overview

As a Layer 2 management protocol, the Spanning Tree Protocol (STP) eliminates Layer 2 loops by selectively blocking redundant links in a network, and in the mean time, allows for link redundancy.

Like many other protocols, STP evolves as the network grows. The later versions of STP are Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP). This chapter describes the characteristics of STP, RSTP, and MSTP and the relationship among them.

Spanning Tree Protocol Overview

Why STP

Spanning tree protocol (STP) is a protocol conforming to IEEE 802.1d. It aims to eliminate loops on data link layer in a local area network (LAN). Devices running this protocol detect loops in the network by exchanging packets with one another and eliminate the loops detected by blocking specific ports until the network is pruned into one with a tree topology. As a network with a tree topology is loop-free, STP prevents packets in it from being duplicated and forwarded endlessly and prevents device and network performance degradation caused by data loops.

In the narrow sense, STP refers to IEEE 802.1d STP; in the broad sense, STP refers to the IEEE 802.1d STP and various enhanced spanning tree protocols derived from that protocol.

Protocol Packets of STP

STP uses bridge protocol data units (BPDUs), also known as configuration messages, as its protocol packets.

STP identifies the network topology by transmitting BPDUs between STP compliant network devices, typically switches and routers. BPDUs contain sufficient information for the network devices to complete the spanning tree calculation.

In STP, BPDUs come in two types:

- Configuration BPDUs, used to calculate spanning trees and maintain the spanning tree topology.
- Topology change notification (TCN) BPDUs, used to notify concerned devices of network topology changes, if any.

Basic concepts in STP

1) Root bridge

A tree network must have a root; hence the concept of **root bridge** has been introduced in STP.

There is one and only one root bridge in an entire STP-based network at a given time. But the root bridge can change because of with changes of the network topology. Therefore, the root bridge is not fixed.

Upon initialization of a network, each device generates and sends out BPDUs periodically with itself as the root bridge; after network convergence, only the root bridge generates and sends out configuration BPDUs at a certain interval, and the other devices just forward the BPDUs.

2) Root port

On a non-root bridge device, the root port is the port with the lowest path cost to the root bridge. The root port is used for communicating with the root bridge. A non-root-bridge device has one and only one root port. The root bridge has no root port.

3) Designated bridge and designated port

Refer to the following table for the description of designated bridge and designated port.

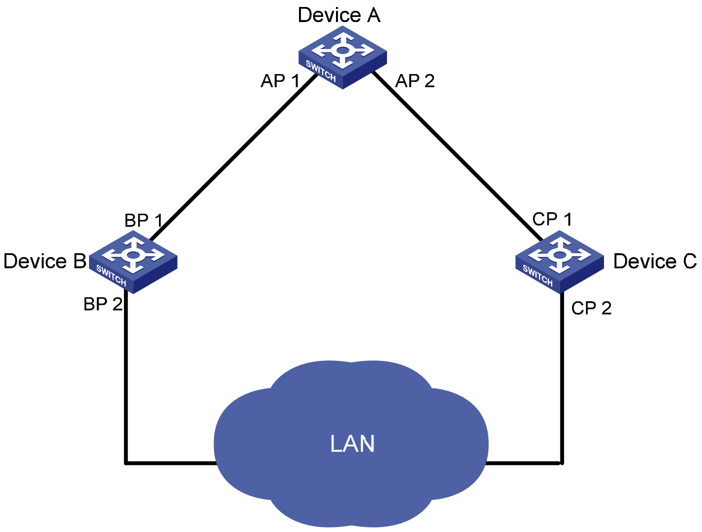
Table 1-1 Designated bridge and designated port

Classification	Designated bridge	Designated port
For a device	A designated bridge is a device that is directly connected to a switch and is responsible for forwarding BPDUs to this switch.	The port through which the designated bridge forwards BPDUs to this device
For a LAN	A designated bridge is a device responsible for forwarding BPDUs to this LAN segment.	The port through which the designated bridge forwards BPDUs to this LAN segment

Figure 1-1 shows designated bridges and designated ports. In the figure, AP1 and AP2, BP1 and BP2, and CP1 and CP2 are ports on Device A, Device B, and Device C respectively.

- If Device A forwards BPDUs to Device B through AP1, the designated bridge for Device B is Device A, and the designated port is the port AP1 on Device A.
- Two devices are connected to the LAN: Device B and Device C. If Device B forwards BPDUs to the LAN, the designated bridge for the LAN is Device B, and the designated port is the port BP2 on Device B.

Figure 1-1 A schematic diagram of designated bridges and designated ports



Note

All the ports on the root bridge are designated ports.

---

4) Bridge ID

A bridge ID consists of eight bytes, where the first two bytes represent the bridge priority of the device, and the latter six bytes represent the MAC address of the device.

Note

The default bridge priority of a 3Com switch 4500 is 32768. You can use a command to configure the bridge priority of a device. For details, see Configuring the Bridge Priority of the Current Switch.

---

5) Path cost

STP uses path costs to indicate the quality of links. A small path cost indicates a higher link quality. The path cost of a port is related to the rate of the link connecting the port. The higher the link rate, the smaller the path cost.

By comparing the path costs of different links, STP selects the most robust links and blocks the other links to prune the network into a tree.

Note

The 3Com switches 4500 support using multiple standards to calculate the path costs of ports, as well as using commands to configure the path costs of ports. For details, see Configuring the Path Cost for a Port.

---

6) Port ID

A port ID used on a 3Com switch 4500 consists of two bytes, that is, 16 bits, where the first six bits represent the port priority, and the latter ten bits represent the port number.

Note

The default priority of all Ethernet ports on 3Com switches 4500 is 128. You can use commands to configure port priorities. For details, see Configuring Port Priority.

How STP works

STP identifies the network topology by transmitting configuration BPDUs between network devices. Configuration BPDUs contain sufficient information for network devices to complete the spanning tree calculation. Important fields in a configuration BPDU include:

- Root bridge ID, consisting of root bridge priority and MAC address.
- Root path cost, the cost of the shortest path to the root bridge.
- Designated bridge ID, designated bridge priority plus MAC address.
- Designated port ID, designated port priority plus port number.
- Message age: lifetime for the configuration BPDUs to be propagated within the network.
- Max age, lifetime for the configuration BPDUs to be kept in a switch.
- Hello time, configuration BPDU interval.
- Forward delay, forward delay of the port.

Note

The implementation of the STP algorithm involves only the following four parts of a configuration BPDU:

- Root bridge ID
- Root path cost
- Designated bridge ID
- Designated port ID

1) Detailed calculation process of the STP algorithm

- Initial state

Upon initialization of a device, each device generates a BPDU with itself as the root bridge, in which the root path cost is 0, designated bridge ID is the device ID, and the designated port is the local port.

- Selection of the optimum configuration BPDU

Each device sends out its configuration BPDU and receives configuration BPDUs from other devices.

The process of selecting the optimum configuration BPDU is as follows:

Table 1-2 Selection of the optimum configuration BPDU

Step	Description
1	Upon receiving a configuration BPDU on a port, the device performs the following processing: • If the received configuration BPDU has a lower priority than that of the configuration BPDU generated by the port, the device will discard the received configuration BPDU without doing any processing on the configuration BPDU of this port. • If the received configuration BPDU has a higher priority than that of the configuration BPDU generated by the port, the device will replace the content of the configuration BPDU generated by the port with the content of the received configuration BPDU.
2	The device compares the configuration BPDUs of all the ports and chooses the optimum configuration BPDU.

Note

Principles for configuration BPDU comparison:

- The configuration BPDU that has the lowest root bridge ID has the highest priority.
- If all configuration BPDUs have the same root bridge ID, they will be compared for their root path costs. If the root path cost in a configuration BPDU plus the path cost corresponding to this port is S, the configuration BPDU with the smallest S value has the highest priority.
- If all configuration BPDUs have the same root path cost, the following fields are compared sequentially: designated bridge IDs, designated port IDs, and then the IDs of the ports on which the configuration BPDUs are received. The smaller these values, the higher priority for the configuration BPDU.

- Selection of the root bridge

At network initialization, each STP-compliant device on the network assumes itself to be the root bridge, with the root bridge ID being its own bridge ID. By exchanging configuration BPDUs, the devices compare one another’s configuration BPDU priority. The device with the highest configuration BPDU priority is elected as the root bridge.

- Selection of the root port and designated ports

The process of selecting the root port and designated ports is as follows:

Table 1-3 Selection of the root port and designated ports

Step	Description
1	A non-root-bridge device takes the port on which the optimum configuration BPDU was received as the root port.
2	Based on the configuration BPDU and the path cost of the root port, the device calculates a designated port configuration BPDU for each of the rest ports. • The root bridge ID is replaced with that of the configuration BPDU of the root port. • The root path cost is replaced with that of the configuration BPDU of the root port plus the path cost corresponding to the root port. • The designated bridge ID is replaced with the ID of this device. • The designated port ID is replaced with the ID of this port.

Step	Description
3	The device compares the calculated configuration BPDU with the configuration BPDU on the port whose role is to be determined, and acts as follows based on the comparison result: • If the calculated configuration BPDU is superior, this port will serve as the designated port, and the configuration BPDU on the port will be replaced with the calculated configuration BPDU, which will be sent out periodically. • If the configuration BPDU on the port is superior, the device stops updating the configuration BPDUs of the port and blocks the port, so that the port only receives configuration BPDUs, but does not forward data or send configuration BPDUs.

Note

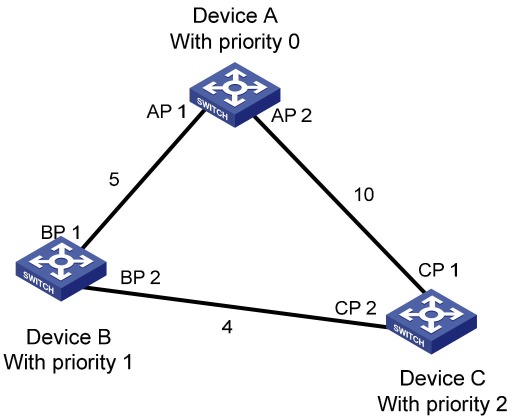
When the network topology is stable, only the root port and designated ports forward traffic, while other ports are all in the blocked state – they only receive STP packets but do not forward user traffic.

Once the root bridge, the root port on each non-root bridge, and designated ports have been successfully elected, the entire tree-shaped topology has been constructed. At this stage, "STP convergence" is complete.

2) Example of how the STP algorithm works

The following is an example of how the STP algorithm works. The specific network diagram is shown in Figure 1-2. The priority of Device A is 0, the priority of Device B is 1, the priority of Device C is 2, and the path costs of these links are 5, 10 and 4 respectively.

Figure 1-2 Network diagram for STP algorithm



- Initial state of each device

The following table shows the initial state of each device.

Table 1-4 Initial state of each device

Device	Port name	BPDU of port
Device A	AP1	{0, 0, 0, AP1}
	AP2	{0, 0, 0, AP2}

Device	Port name	BPDU of port
Device B	BP1	{1, 0, 1, BP1}
	BP2	{1, 0, 1, BP2}
Device C	CP1	{2, 0, 2, CP1}
	CP2	{2, 0, 2, CP2}

- Comparison process and result on each device

The following table shows the comparison process and result on each device.

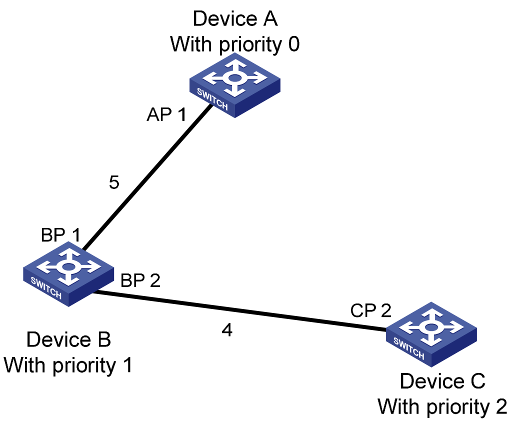
Table 1-5 Comparison process and result on each device

Device	Comparison process	BPDU of port after comparison
Device A	• Port AP1 receives the configuration BPDU of Device B {1, 0, 1, BP1}. Device A finds that the configuration BPDU of the local port {0, 0, 0, AP1} is superior to the configuration received message, and discards the received configuration BPDU. • Port AP2 receives the configuration BPDU of Device C {2, 0, 2, CP1}. Device A finds that the BPDU of the local port {0, 0, 0, AP2} is superior to the received configuration BPDU, and discards the received configuration BPDU. • Device A finds that both the root bridge and designated bridge in the configuration BPDUs of all its ports are Device A itself, so it assumes itself to be the root bridge. In this case, it does not make any change to the configuration BPDU of each port, and starts sending out configuration BPDUs periodically.	AP1: {0, 0, 0, AP1} AP2: {0, 0, 0, AP2}
Device B	• Port BP1 receives the configuration BPDU of Device A {0, 0, 0, AP1}. Device B finds that the received configuration BPDU is superior to the configuration BPDU of the local port {1, 0,1, BP1}, and updates the configuration BPDU of BP1. • Port BP2 receives the configuration BPDU of Device C {2, 0, 2, CP2}. Device B finds that the configuration BPDU of the local port {1, 0, 1, BP2} is superior to the received configuration BPDU, and discards the received configuration BPDU.	BP1: {0, 0, 0, AP1} BP2: {1, 0, 1, BP2}
	• Device B compares the configuration BPDUs of all its ports, and determines that the configuration BPDU of BP1 is the optimum configuration BPDU. Then, it uses BP1 as the root port, the configuration BPDUs of which will not be changed. • Based on the configuration BPDU of BP1 and the path cost of the root port (5), Device B calculates a designated port configuration BPDU for BP2 {0, 5, 1, BP2}. • Device B compares the calculated configuration BPDU {0, 5, 1, BP2} with the configuration BPDU of BP2. If the calculated BPDU is superior, BP2 will act as the designated port, and the configuration BPDU on this port will be replaced with the calculated configuration BPDU, which will be sent out periodically.	Root port BP1: {0, 0, 0, AP1} Designated port BP2: {0, 5, 1, BP2}

Device	Comparison process	BPDU of port after comparison
Device C	• Port CP1 receives the configuration BPDU of Device A {0, 0, 0, AP2}. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP1}, and updates the configuration BPDU of CP1. • Port CP2 receives the configuration BPDU of port BP2 of Device B {1, 0, 1, BP2} before the message was updated. Device C finds that the received configuration BPDU is superior to the configuration BPDU of the local port {2, 0, 2, CP2}, and updates the configuration BPDU of CP2.	CP1: {0, 0, 0, AP2} CP2: {1, 0, 1, BP2}
	By comparison: • The configuration BPDUs of CP1 is elected as the optimum configuration BPDU, so CP1 is identified as the root port, the configuration BPDUs of which will not be changed. • Device C compares the calculated designated port configuration BPDU {0, 10, 2, CP2} with the configuration BPDU of CP2, and CP2 becomes the designated port, and the configuration BPDU of this port will be replaced with the calculated configuration BPDU.	Root port CP1: {0, 0, 0, AP2} Designated port CP2: {0, 10, 2, CP2}
	• Next, port CP2 receives the updated configuration BPDU of Device B {0, 5, 1, BP2}. Because the received configuration BPDU is superior to its old one, Device C launches a BPDU update process. • At the same time, port CP1 receives configuration BPDUs periodically from Device A. Device C does not launch an update process after comparison.	CP1: {0, 0, 0, AP2} CP2: {0, 5, 1, BP2}
	By comparison: • Because the root path cost of CP2 (9) (root path cost of the BPDU (5) + path cost corresponding to CP2 (4)) is smaller than the root path cost of CP1 (10) (root path cost of the BPDU (0) + path cost corresponding to CP2 (10)), the BPDU of CP2 is elected as the optimum BPDU, and CP2 is elected as the root port, the messages of which will not be changed. • After comparison between the configuration BPDU of CP1 and the calculated designated port configuration BPDU, port CP1 is blocked, with the configuration BPDU of the port remaining unchanged, and the port will not receive data from Device A until a spanning tree calculation process is triggered by a new condition, for example, the link from Device B to Device C becomes down.	Blocked port CP2: {0, 0, 0, AP2} Root port CP2: {0, 5, 1, BP2}

After the comparison processes described in the table above, a spanning tree with Device A as the root bridge is stabilized, as shown in Figure 1-3.

Figure 1-3 The final calculated spanning tree



Note

To facilitate description, the spanning tree calculation process in this example is simplified, while the actual process is more complicated.

3) The BPDU forwarding mechanism in STP

- Upon network initiation, every switch regards itself as the root bridge, generates configuration BPDUs with itself as the root, and sends the configuration BPDUs at a regular interval of hello time.
- If it is the root port that received the configuration BPDU and the received configuration BPDU is superior to the configuration BPDU of the port, the device will increase message age carried in the configuration BPDU by a certain rule and start a timer to time the configuration BPDU while it sends out this configuration BPDU through the designated port.
- If the configuration BPDU received on the designated port has a lower priority than the configuration BPDU of the local port, the port will immediately sends out its better configuration BPDU in response.
- If a path becomes faulty, the root port on this path will no longer receive new configuration BPDUs and the old configuration BPDUs will be discarded due to timeout. In this case, the device generates configuration BPDUs with itself as the root bridge and sends configuration BPDUs and TCN BPDUs. This triggers a new spanning tree calculation so that a new path is established to restore the network connectivity.

However, the newly calculated configuration BPDU will not be propagated throughout the network immediately, so the old root ports and designated ports that have not detected the topology change continue forwarding data through the old path. If the new root port and designated port begin to forward data as soon as they are elected, a temporary loop may occur.

4) STP timers

The following three time parameters are important for STP calculation:

- Forward delay, the period a device waits before state transition.

A link failure triggers a new round of spanning tree calculation and results in changes of the spanning tree. However, as new configuration BPDUs cannot be propagated throughout the network immediately, if the new root port and designated port begin to forward data as soon as they are elected, loops may temporarily occur.

For this reason, the protocol uses a state transition mechanism. Namely, a newly elected root port and the designated ports must go through a period, which is twice the forward delay time, before they transit to the forwarding state. The period allows the new configuration BPDUs to be propagated throughout the entire network.

- Hello time, the interval for sending hello packets. Hello packets are used to check link state.

A switch sends hello packets to its neighboring devices at a regular interval (the hello time) to check whether the links are faulty.

- Max time, lifetime of the configuration BPDUs stored in a switch. A configuration BPDU that has "expired" is discarded by the switch.

Rapid Spanning Tree Protocol Overview

Rapid spanning tree protocol (RSTP) is an optimized version of STP. RSTP allows a newly elected root port or designated port to enter the forwarding state much quicker under certain conditions than in STP. As a result, it takes a shorter time for the network to reach the final topology stability.

Note

- In RSTP, the state of a root port can transit fast under the following conditions: the old root port on the device has stopped forwarding data and the upstream designated port has started forwarding data.
- In RSTP, the state of a designated port can transit fast under the following conditions: the designated port is an edge port or a port connected with a point-to-point link. If the designated port is an edge port, it can enter the forwarding state directly; if the designated port is connected with a point-to-point link, it can enter the forwarding state immediately after the device undergoes handshake with the downstream device and gets a response.

Multiple Spanning Tree Protocol Overview

Why MSTP

1) Disadvantages of STP and RSTP

STP does not support rapid state transition of ports. A newly elected root port or designated port must wait twice the forward delay time before transiting to the forwarding state, even if it is a port on a point-to-point link or it is an edge port (an edge port refers to a port that directly connects to a user terminal rather than to another device or a shared LAN segment.)

RSTP supports rapid convergence. Like STP, it is of the following disadvantages: all bridges in a LAN are on the same spanning tree; redundant links cannot be blocked by VLAN; the packets of all VLANs are forwarded along the same spanning tree.

2) Features of MSTP

The multiple spanning tree protocol (MSTP) overcomes the shortcomings of STP and RSTP. In addition to support for rapid network convergence, it also allows data flows of different VLANs to be forwarded along their own paths, thus providing a better load sharing mechanism for redundant links.

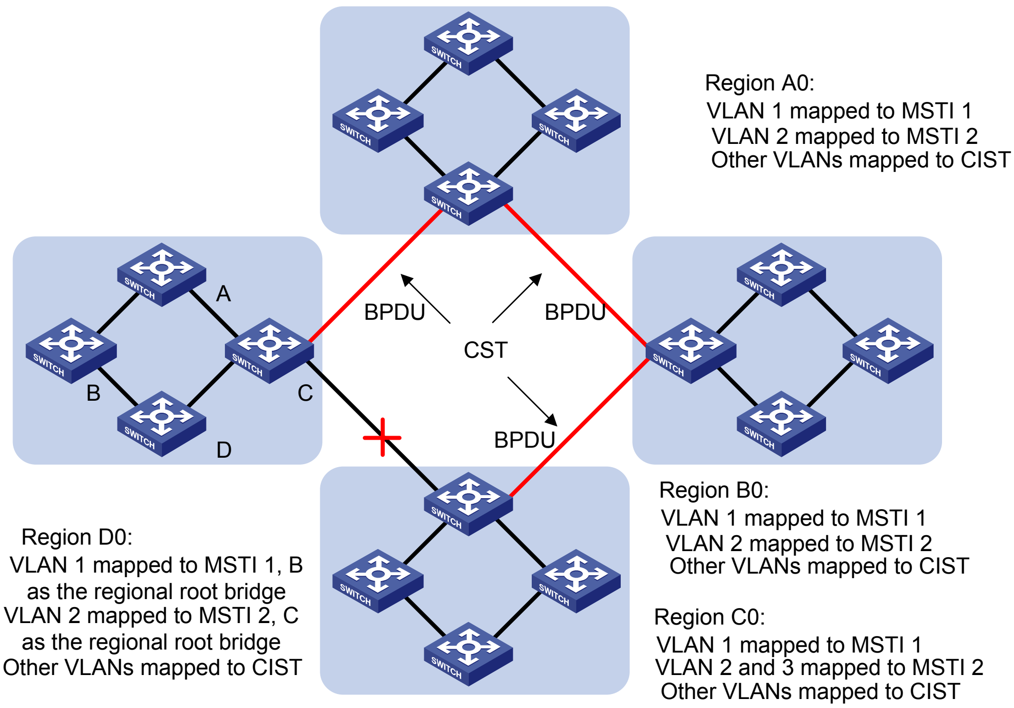
MSTP features the following:

- MSTP supports mapping VLANs to Multiple Spanning Tree (MST) instances (MSTIs) by means of a VLAN-to-instance mapping table. MSTP introduces **instances** (which integrates multiple VLANs into a set) and can bind multiple VLANs to an instance, thus saving communication overhead and improving resource utilization.
- MSTP divides a switched network into multiple regions, each containing multiple spanning trees that are independent of one another.
- MSTP prunes a ring network into a network with tree topology, preventing packets from being duplicated and forwarded in a network endlessly. Furthermore, it offers multiple redundant paths for forwarding data, and thus achieves load balancing for forwarding VLAN data.
- MSTP is compatible with STP and RSTP.

Basic MSTP Terminology

Figure 1-4 illustrates basic MSTP terms (assuming that MSTP is enabled on each switch in this figure).

Figure 1-4 Basic MSTP terminologies



1) MST region

A multiple spanning tree region (MST region) comprises multiple physically-interconnected MSTP-enabled switches and the corresponding network segments connected to these switches. These switches have the same region name, the same VLAN-to-instance mapping configuration and the same MSTP revision level.

A switched network can contain multiple MST regions. You can group multiple switches into one MST region by using the corresponding MSTP configuration commands.

As shown in Figure 1-4, all the switches in region A0 are of the same MST region-related configuration, including:

- Region name
- VLAN-to-instance mapping (that is, VLAN 1 is mapped to MSTI 1, VLAN 2 is mapped to MSTI 2, and the other VLANs are mapped to CIST.)
- MSTP revision level (not shown in Figure 1-4)

2) MSTI

A multiple spanning tree instance (MSTI) refers to a spanning tree in an MST region.

Multiple spanning trees can be established in one MST region. These spanning trees are independent of each other. For example, each region in Figure 1-4 contains multiple spanning trees known as MSTIs. Each of these spanning trees corresponds to a VLAN.

3) VLAN-to-instance mapping table

A VLAN-to-instance mapping table is maintained for each MST region. The table is a collection of mappings between VLANs and MSTIs. For example, in Figure 1-4, the VLAN-to-instance mapping table of region A0 contains these mappings: VLAN 1 to MSTI 1; VLAN 2 to MSTI 2, and other VLANs to CIST. In an MST region, load balancing is implemented according to the VLAN-to-instance mapping table.

4) IST

An internal spanning tree (IST) is a spanning tree in an MST region.

ISTs together with the common spanning tree (CST) form the common and internal spanning tree (CIST) of the entire switched network. An IST is a special MSTI; it is a branch of CIST in the MST region.

In Figure 1-4, each MST region has an IST, which is a branch of the CIST.

5) CST

A common spanning tree (CST) is a single spanning tree in a switched network that connects all MST regions in the network. If you regard each MST region in the network as a “switch”, then the CST is the spanning tree generated by STP or RSTP running on the "switches". For example, the red lines in Figure 1-4 represent the CST.

6) CIST

A common and internal spanning tree (CIST) is the spanning tree in a switched network that connects all switches in the network. It comprises the ISTs and the CST.

In Figure 1-4, the ISTs in the MST regions and the CST connecting the MST regions form the CIST.

7) Region root

A region root is the root of the IST or an MSTI in an MST region. Different spanning trees in an MST region may have different topologies and thus have different region roots.

In region D0 shown in Figure 1-4, the region root of MSTI 1 is switch B, and the region root of MSTI 2 is switch C.

8) Common root bridge

The common root bridge is the root of the CIST. The common root bridge of the network shown in Figure 1-4 is a switch in region A0.

9) Port role

MSTP calculation involves the following port roles: root port, designated port, master port, region boundary port, alternate port, and backup port.

- A root port is used to forward packets to the root.
- A designated port is used to forward packets to a downstream network segment or switch.
- A master port connects an MST region to the common root. The path from the master port to the common root is the shortest path between the MST region and the common root. In the CST, the master port is the root port of the region, which is considered as a node. The master port is a special boundary port. It is a root port in the IST/CIST while a master port in the other MSTIs.

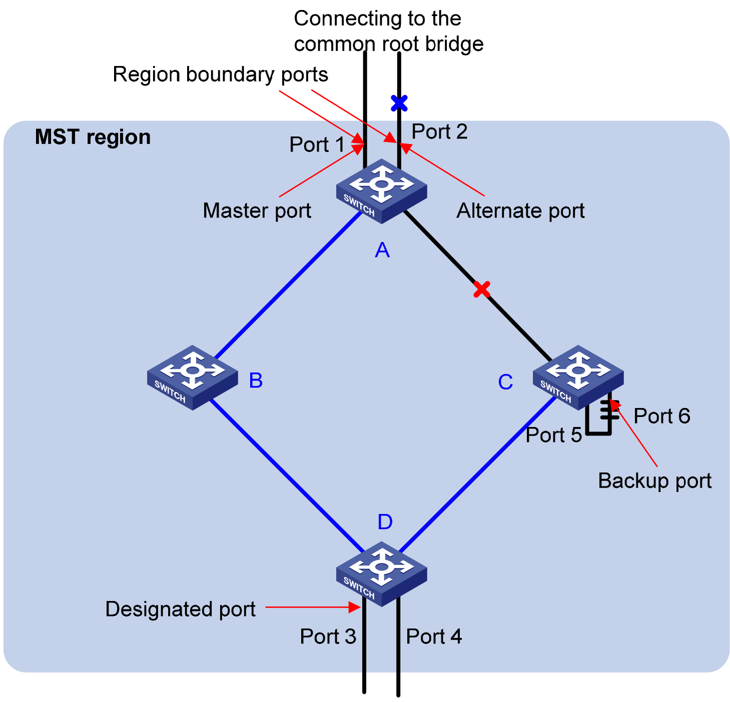
- A region boundary port is located on the boundary of an MST region and is used to connect one MST region to another MST region, an STP-enabled region or an RSTP-enabled region.
- An alternate port is a secondary port of a root port or master port and is used for rapid transition. With the root port or master port being blocked, the alternate port becomes the new root port or master port.
- A backup port is the secondary port of a designated port and is used for rapid transition. With the designated port being blocked, the backup port becomes the new designated port fast and begins to forward data seamlessly. When two ports of an MSTP-enabled switch are interconnected, the switch blocks one of the two ports to eliminate the loop that occurs. The blocked port is the backup port.

In Figure 1-5, switch A, switch B, switch C, and switch D form an MST region. Port 1 and port 2 on switch A connect upstream to the common root. Port 5 and port 6 on switch C form a loop. Port 3 and port 4 on switch D connect downstream to other MST regions. This figure shows the roles these ports play.

Note

- A port can play different roles in different MSTIs.
- The role a region boundary port plays in an MSTI is consistent with the role it plays in the CIST. The master port, which is a root port in the CIST while a master port in the other MSTIs, is an exception.
- For example, in Figure 1-5, port 1 on switch A is a region boundary port. It is a root port in the CIST while a master port in all the other MSTIs in the region.

Figure 1-5 Port roles



10) Port state

In MSTP, a port can be in one of the following three states:

- Forwarding state. Ports in this state can forward user packets and receive/send BPDU packets.
- Learning state. Ports in this state can receive/send BPDU packets but do not forward user packets.
- Discarding state. Ports in this state can only receive BPDU packets.

Port roles and port states are not mutually dependent. Table 1-6 lists possible combinations of port states and port roles.

Table 1-6 Combinations of port states and port roles

Port role / Port state	Root/master port	Designated port	Region Boundary port	Alternate port	Backup port
Forwarding	√	√	√	—	—
Learning	√	√	√	—	—
Discarding	√	√	√	√	√

Principle of MSTP

MSTP divides a Layer 2 network into multiple MST regions. The CSTs are generated between these MST regions, and multiple spanning trees (also called MSTIs) can be generated in each MST region. As well as RSTP, MSTP uses configuration BPDUs for spanning tree calculation. The only difference is that the configuration BPDUs for MSTP carry the MSTP configuration information on the switches.

1) Calculate the CIST

Through comparing configuration BPDUs, the switch of the highest priority in the network is selected as the root of the CIST. In each MST region, an IST is calculated by MSTP. At the same time, MSTP regards each MST region as a switch to calculate the CSTs of the network. The CSTs, together with the ISTs, form the CIST of the network.

2) Calculate an MSTI

Within an MST region, MSTP generates different MSTIs for different VLANs based on the VLAN-to-instance mappings. MSTP performs a separate calculation process, which is similar to spanning tree calculation in STP, for each spanning tree. For details, refer to How STP works.

In MSTP, a VLAN packet is forwarded along the following paths:

- Within an MST region, the packet is forwarded along the corresponding MSTI.
- Between two MST regions, the packet is forwarded along the CST.

MSTP Implementation on Switches

MSTP is compatible with both STP and RSTP. That is, MSTP-enabled switches can recognize the protocol packets of STP and RSTP and use them for their respective spanning tree calculation.

The 3com switches 4500 support MSTP. After MSTP is enabled on a switch 4500, the switch operates in MSTP mode by default. If the network contains switches that run the STP/RSTP protocol, you can use commands to configure the switches 4500 to operate in STP-compatible mode or RSTP-compatible mode (see Configuring the MSTP Operation Mode for more information):

- In STP-compatible mode, all ports of the switches 4500 send out STP BPDUs
- In RSTP mode, all ports of the switches 4500 send out RSTP BPDUs.

In addition to the basic MSTP functions, 3com Switch 4500 also provides the following functions for users to manage their switches.

- Root bridge hold
- Root bridge backup
- Root guard
- BPDU guard
- Loop guard
- TC-BPDU attack guard

Protocols and Standards

MSTP is documented in:

- IEEE 802.1D: spanning tree protocol
- IEEE 802.1w: rapid spanning tree protocol
- IEEE 802.1s: multiple spanning tree protocol

MSTP Configuration Task List

Before configuring MSTP, you need to know the position of each device in each MSTI: root bridge or leave node. In each MSTI, one, and only one device acts as the root bridge, while all others as leaf nodes.

Complete these tasks to configure MSTP:

Task		Remarks
Configuring Root Bridge	Enabling MSTP	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after other related configurations are performed.
	Configuring an MST Region	Required
	Specifying the Current Switch as a Root Bridge/Secondary Root Bridge	Required
	Configuring the Bridge Priority of the Current Switch	Optional The priority of a switch cannot be changed after the switch is specified as the root bridge or a secondary root bridge.
	Configuring How a Port Recognizes and Sends MSTP Packets	Optional
	Configuring the MSTP Operation Mode	Optional
	Configuring the Maximum Hop Count of an MST Region	Optional
	Configuring the Network Diameter of the Switched Network	Optional The default value is recommended.
	Configuring the MSTP Time-related Parameters	Optional The default values are recommended.
	Configuring the Timeout Time Factor	Optional

Task		Remarks
	Configuring the Maximum Transmitting Rate on the Current Port	Optional The default value is recommended.
	Configuring the Current Port as an Edge Port	Optional
	Setting the Link Type of a Port to P2P	Optional
Configuring Leaf Nodes	Enabling MSTP	Required To prevent network topology jitter caused by other related configurations, you are recommended to enable MSTP after performing other configurations.
	Configuring an MST Region	Required
	Configuring How a Port Recognizes and Sends MSTP Packets	Optional
	Configuring the Timeout Time Factor	Optional
	Configuring the Maximum Transmitting Rate on the Current Port	Optional The default value is recommended.
	Configuring the Current Port as an Edge Port	Optional
	Configuring the Path Cost for a Port	Optional
	Configuring Port Priority	Optional
	Setting the Link Type of a Port to P2P	Optional
Performing mCheck Operation		Optional
Configuring Guard Functions		Optional
Configuring Digest Snooping		Optional
Configuring Rapid Transition		Optional
错误！未找到引用源。		Optional
MSTP Maintenance Configuration		Optional
Enabling Trap Messages Conforming to 802.1d Standard		Optional

Configuring Root Bridge

Configuring an MST Region

Configuration procedure

Follow these steps to configure an MST region:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter MST region view	**stp region-configuration**	—

To do...	Use the command...	Remarks
Configure the name of the MST region	**region-name** *name*	Required The default MST region name of a switch is its MAC address.
Configure the VLAN-to-instance mapping table for the MST region	**instance** *instance-id* **vlan** *vlan-list*	Required Both commands can be used to configure VLAN-to-instance mapping tables. By default, all VLANs in an MST region are mapped to MSTI 0.
	vlan-mapping modulo *modulo*	
Configure the MSTP revision level for the MST region	**revision-level** *level*	Required The default revision level of an MST region is level 0.
Activate the configuration of the MST region manually	**active region-configuration**	Required
Display the configuration of the current MST region	**check region-configuration**	Optional
Display the currently valid configuration of the MST region	**display stp region-configuration**	Available in any view

Note

Neighbor Topology Discovery Protocol (NTDP) packets sent by devices in a cluster can only be transmitted within the MSTI where the management VLAN of the cluster resides. For more information about clusters and the NTDP protocol, see *Cluster Operation*.

Configuring MST region-related parameters (especially the VLAN-to-instance mapping table) results in spanning tree recalculation and network topology jitter. To reduce network topology jitter caused by the configuration, MSTP does not recalculate spanning trees immediately after the configuration; it does this only after you perform one of the following operations, and then the configuration can really takes effect:

- Activate the new MST region-related settings by using the **active region-configuration** command
- Enable MSTP by using the **stp enable** command

Note

- MSTP-enabled switches are in the same region only when they have the same format selector (a 802.1s-defined protocol selector, which is 0 by default and cannot be configured), MST region name, VLAN-to-instance mapping table, and revision level.
- The 3Com switches 4500 support only the MST region name, VLAN-to-instance mapping table, and revision level. Switches with the settings of these parameters being the same are assigned to the same MST region.

Configuration example

Configure an MST region named **info**, the MSTP revision level being level 1, VLAN 2 through VLAN 10 being mapped to MSTI 1, and VLAN 20 through VLAN 30 being mapped to MSTI 2.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name info
[Sysname-mst-region] instance 1 vlan 2 to 10
[Sysname-mst-region] instance 2 vlan 20 to 30
[Sysname-mst-region] revision-level 1
[Sysname-mst-region] active region-configuration
```

Verify the above configuration.

```
[Sysname-mst-region] check region-configuration
Admin configuration
   Format selector    :0
   Region name        :info
   Revision level     :1

   Instance   Vlans Mapped
      0       1, 11 to 19, 31 to 4094
      1       2 to 10
      2       20 to 30
```

Specifying the Current Switch as a Root Bridge/Secondary Root Bridge

MSTP can automatically choose a switch as a root bridge through calculation. You can also manually specify the current switch as a root bridge by using the corresponding commands.

Specify the current switch as the root bridge of a spanning tree

Follow these steps to specify the current switch as the root bridge of a spanning tree:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Specify the current switch as the root bridge of a spanning tree	**stp** [**instance** *instance-id*] **root primary** [**bridge-diameter** *bridgenumber* [**hello-time** *centi-seconds*]]	Required

Specify the current switch as the secondary root bridge of a spanning tree

Follow these steps to specify the current switch as the secondary root bridge of a spanning tree:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Specify the current switch as the secondary root bridge of a specified spanning tree	**stp** [**instance** *instance-id*] **root secondary** [**bridge-diameter** *bridgenumber* [**hello-time** *centi-seconds*]]	Required

Using the **stp root primary/stp root secondary** command, you can specify the current switch as the root bridge or the secondary root bridge of the MSTI identified by the *instance-id* argument. If the value of the *instance-id* argument is set to 0, the **stp root primary/stp root secondary** command specify the current switch as the root bridge or the secondary root bridge of the CIST.

A switch can play different roles in different MSTIs. That is, it can be the root bridges in an MSTI and be a secondary root bridge in another MSTI at the same time. But in the same MSTI, a switch cannot be the root bridge and the secondary root bridge simultaneously.

When the root bridge fails or is turned off, the secondary root bridge becomes the root bridge if no new root bridge is configured. If you configure multiple secondary root bridges for an MSTI, the one with the smallest MAC address replaces the root bridge when the latter fails.

You can specify the network diameter and the hello time parameters while configuring a root bridge/secondary root bridge. Refer to Configuring the Network Diameter of the Switched Network and Configuring the MSTP Time-related Parameters for information about the network diameter parameter and the hello time parameter.

Note

- You can configure a switch as the root bridges of multiple MSTIs. But you cannot configure two or more root bridges for one MSTI. So, do not configure root bridges for the same MSTI on two or more switches using the **stp root primary** command.
- You can configure multiple secondary root bridges for one MSTI. That is, you can configure secondary root bridges for the same MSTI on two or more switches using the **stp root secondary** command.
- You can also configure the current switch as the root bridge by setting the priority of the switch to 0. Note that once a switch is configured as the root bridge or a secondary root bridge, its priority cannot be modified.

Configuration example

Configure the current switch as the root bridge of MSTI 1 and a secondary root bridge of MSTI 2.

```
<Sysname> system-view
[Sysname] stp instance 1 root primary
[Sysname] stp instance 2 root secondary
```

Configuring the Bridge Priority of the Current Switch

Root bridges are selected according to the bridge priorities of switches. You can make a specific switch be selected as a root bridge by setting a lower bridge priority for the switch. An MSTP-enabled switch can have different bridge priorities in different MSTIs.

Configuration procedure

Follow these steps to configure the bridge priority of the current switch:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—

To do...	Use the command...	Remarks
Set the bridge priority for the current switch	**stp** [**instance** *instance-id*] **priority** *priority*	Required The default bridge priority of a switch is 32,768.

Caution

- Once you specify a switch as the root bridge or a secondary root bridge by using the **stp root primary** or **stp root secondary** command, the bridge priority of the switch cannot be configured any more.
- During the selection of the root bridge, if multiple switches have the same bridge priority, the one with the smallest MAC address becomes the root bridge.

Configuration example

Set the bridge priority of the current switch to 4,096 in MSTI 1.

```
<Sysname> system-view
[Sysname] stp instance 1 priority 4096
```

Configuring How a Port Recognizes and Sends MSTP Packets

A port can send/recognize MSTP packets of two formats:

- **dot1s**: 802.1s-compliant standard format
- **legacy**: Compatible format

By default, the packet format recognition mode of a port is **auto**, namely the port automatically distinguishes the two MSTP packet formats, and determines the format of packets it will send based on the recognized format. You can configure the MSTP packet format to be used by a port. After the configuration, when working in MSTP mode, the port sends and receives only MSTP packets of the format you have configured to communicate with devices that send packets of the same format.

Configuration procedure

Follow these steps to configure how a port recognizes and sends MSTP packets (in system view):

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure how a port recognizes and sends MSTP packets	**stp interface** *interface-list* **compliance** { **auto** | **dot1s** | **legacy** }	Required By default, a port recognizes and sends MSTP packets in the automatic mode. That is, it determines the format of packets to be sent according to the format of the packets received.

Follow these steps to configure how a port recognizes and sends MSTP packets (in Ethernet port view):

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure how a port recognizes and sends MSTP packets	**stp compliance** { **auto** | **dot1s** | **legacy** }	Required By default, a port recognizes and sends MSTP packets in the automatic mode. That is, it determines the format of packets to be sent according to the format of the packets received.

Configuration example

Configure Ethernet 1/0/1 to recognize and send packets in dot1s format.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp compliance dot1s
```

Restore the default mode for Ethernet 1/0/1 to recognize/send MSTP packets.

```
[Sysname-Ethernet1/0/1] undo stp compliance
```

Configuring the MSTP Operation Mode

To make an MSTP-enabled switch compatible with STP/RSTP, MSTP provides the following three operation modes:

- STP-compatible mode, where the ports of a switch send STP BPDUs to neighboring devices. If STP-enabled switches exist in a switched network, you can use the **stp mode stp** command to configure an MSTP-enabled switch to operate in STP-compatible mode.
- RSTP-compatible mode, where the ports of a switch send RSTP BPDUs to neighboring devices. If RSTP-enabled switches exist in a switched network, you can use the **stp mode rstp** command to configure an MSTP-enabled switch to operate in RSTP-compatible mode.
- MSTP mode, where the ports of a switch send MSTP BPDUs or STP BPDUs (if the switch is connected to STP-enabled switches) to neighboring devices. In this case, the switch is MSTP-capable.

Configuration procedure

Follow these steps to configure the MSTP operation mode:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the MSTP operation mode	**stp mode** { **stp** | **rstp** | **mstp** }	Required An MSTP-enabled switch operates in the MSTP mode by default.

Configuration example

Specify the MSTP operation mode as STP-compatible.

```
<Sysname> system-view
[Sysname] stp mode stp
```

Configuring the Maximum Hop Count of an MST Region

The maximum hop count configured on the region root is also the maximum hops of the MST region. The value of the maximum hop count limits the size of the MST region.

A configuration BPDU contains a field that maintains the remaining hops of the configuration BPDU. And a switch discards the configuration BPDUs whose remaining hops are 0. After a configuration BPDU reaches a root bridge of a spanning tree in an MST region, the value of the remaining hops field in the configuration BPDU is decreased by 1 every time the configuration BPDU passes one switch. Such a mechanism disables the switches that are beyond the maximum hop count from participating in spanning tree calculation, and thus limits the size of an MST region.

With such a mechanism, the maximum hop count configured on the switch operating as the root bridge of the CIST or an MSTI in an MST region becomes the network diameter of the spanning tree, which limits the size of the spanning tree in the current MST region. The switches that are not root bridges in the MST region adopt the maximum hop settings of their root bridges.

Configuration procedure

Follow these steps to configure the maximum hop count for an MST region:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the maximum hop count of the MST region	**stp max-hops** *hops*	Required By default, the maximum hop count of an MST region is 20.

The bigger the maximum hop count, the larger the MST region is. Note that only the maximum hop settings on the switch operating as a region root can limit the size of the MST region.

Configuration example

Configure the maximum hop count of the MST region to be 30.

```
<Sysname> system-view
[Sysname] stp max-hops 30
```

Configuring the Network Diameter of the Switched Network

In a switched network, any two switches can communicate with each other through a specific path made up of multiple switches. The network diameter of a network is measured by the number of switches; it equals the number of the switches on the longest path (that is, the path containing the maximum number of switches).

Configuration procedure

Follow these steps to configure the network diameter of the switched network:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the network diameter of the switched network	**stp bridge-diameter** *bridgenumber*	Required The default network diameter of a network is 7.

The network diameter parameter indicates the size of a network. The bigger the network diameter is, the larger the network size is.

After you configure the network diameter of a switched network, an MSTP-enabled switch adjusts its hello time, forward delay, and max age settings accordingly to better values.

The network diameter setting only applies to CIST; it is invalid for MSTIs.

Configuration example

Configure the network diameter of the switched network to 6.

```
<Sysname> system-view
[Sysname] stp bridge-diameter 6
```

Configuring the MSTP Time-related Parameters

Three MSTP time-related parameters exist: forward delay, hello time, and max age. You can configure the three parameters to control the process of spanning tree calculation.

Configuration procedure

Follow these steps to configure MSTP time-related parameters:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the forward delay parameter	**stp timer forward-delay** *centiseconds*	Required The forward delay parameter defaults to 1,500 centiseconds (namely, 15 seconds).
Configure the hello time parameter	**stp timer hello** *centiseconds*	Required The hello time parameter defaults to 200 centiseconds (namely, 2 seconds).
Configure the max age parameter	**stp timer max-age** *centiseconds*	Required The max age parameter defaults to 2,000 centiseconds (namely, 20 seconds).

All switches in a switched network adopt the three time-related parameters configured on the CIST root bridge.

Caution

- The forward delay parameter and the network diameter are correlated. Normally, a large network diameter corresponds to a large forward delay. A too small forward delay parameter may result in temporary redundant paths. And a too large forward delay parameter may cause a network unable to resume the normal state in time after changes occurred to the network. The default value is recommended.
- An adequate hello time parameter enables a switch to detect link failures in time without occupying too many network resources. And a too small hello time parameter may result in duplicated configuration BPDUs being sent frequently, which increases the work load of the switches and wastes network resources. The default value is recommended.
- As for the max age parameter, if it is too small, network congestion may be falsely regarded as link failures, which results in frequent spanning tree recalculation. If it is too large, link problems may be unable to be detected in time, which prevents spanning trees being recalculated in time and makes the network less adaptive. The default value is recommended.

As for the configuration of the three time-related parameters (that is, the hello time, forward delay, and max age parameters), the following formulas must be met to prevent frequent network jitter.

2 x (forward delay – 1 second) >= max age

Max age >= 2 x (hello time + 1 second)

You are recommended to specify the network diameter of the switched network and the hello time by using the **stp root primary** or **stp root secondary** command. After that, the three proper time-related parameters are determined automatically.

Configuration example

Configure the forward delay parameter to be 1,600 centiseconds, the hello time parameter to be 300 centiseconds, and the max age parameter to be 2,100 centiseconds (assuming that the current switch operates as the CIST root bridge).

```
<Sysname> system-view
[Sysname] stp timer forward-delay 1600
[Sysname] stp timer hello 300
[Sysname] stp timer max-age 2100
```

Configuring the Timeout Time Factor

When the network topology is stable, a non-root-bridge switch regularly forwards BPDUs received from the root bridge to its neighboring devices at the interval specified by the hello time parameter to check for link failures. Normally, a switch regards its upstream switch faulty if the former does not receive any BPDU from the latter in a period three times of the hello time and then initiates the spanning tree recalculation process.

Spanning trees may be recalculated even in a steady network if an upstream switch continues to be busy. You can configure the timeout time factor to a larger number to avoid such cases. Normally, the timeout time can be four or more times of the hello time. For a steady network, the timeout time can be five to seven times of the hello time.

Configuration procedure

Follow these steps to configure the timeout time factor:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the timeout time factor for the switch	**stp timer-factor** *number*	Required The timeout time factor defaults to 3.

For a steady network, the timeout time can be five to seven times of the hello time.

Configuration example

Configure the timeout time factor to be 6.

```
<Sysname> system-view
[Sysname] stp timer-factor 6
```

Configuring the Maximum Transmitting Rate on the Current Port

The maximum transmitting rate of a port specifies the maximum number of configuration BPDUs a port can transmit in a period specified by the hello time parameter. It depends on the physical state of the port and network structure. You can configure this parameter according to the network.

Configure the maximum transmitting rate for specified ports in system view

Follow these steps to configure the maximum transmitting rate for specified ports in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the maximum transmitting rate for specified ports	**stp interface** *interface-list* **transmit-limit** *packetnum*	Required The maximum transmitting rate of all Ethernet ports on a switch defaults to 10.

Configure the maximum transmitting rate in Ethernet port view

Follow these steps to configure the maximum transmitting rate in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the maximum transmitting rate	**stp transmit-limit** *packetnum*	Required The maximum transmitting rate of all Ethernet ports on a switch defaults to 10.

As the maximum transmitting rate parameter determines the number of the configuration BPDUs transmitted in each hello time, set it to a proper value to prevent MSTP from occupying too many network resources. The default value is recommended.

Configuration example

Set the maximum transmitting rate of Ethernet 1/0/1 to 15.

1) Configure the maximum transmitting rate in system view

```
<Sysname> system-view
[Sysname] stp interface Ethernet 1/0/1 transmit-limit 15
```

2) Configure the maximum transmitting rate in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp transmit-limit 15
```

Configuring the Current Port as an Edge Port

Edge ports are ports that neither directly connects to other switches nor indirectly connects to other switches through network segments. After a port is configured as an edge port, the rapid transition mechanism is applicable to the port. That is, when the port changes from the blocking state to the forwarding state, it does not have to wait for a delay.

You can configure a port as an edge port in one of the following two ways.

Configure a port as an edge port in system view

Follow these steps to configure a port as an edge port in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the specified ports as edge ports	**stp interface** *interface-list* **edged-port enable**	Required By default, all the Ethernet ports of a switch are non-edge ports.

Configure a port as an edge port in Ethernet port view

Follow these steps to configure a port as an edge port in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the port as an edge port	**stp edged-port enable**	Required By default, all the Ethernet ports of a switch are non-edge ports.

On a switch with BPDU guard disabled, an edge port becomes a non-edge port again once it receives a BPDU from another port.

Note

You are recommended to configure the Ethernet ports connected directly to terminals as edge ports and enable the BPDU guard function at the same time. This not only enables these ports to turn to the forwarding state rapidly but also secures your network.

Configuration example

Configure Ethernet 1/0/1 as an edge port.

1) Configure Ethernet 1/0/1 as an edge port in system view

```
<Sysname> system-view
[Sysname] stp interface Ethernet 1/0/1 edged-port enable
```

2) Configure Ethernet 1/0/1 as an edge port in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp edged-port enable
```

Setting the Link Type of a Port to P2P

A point-to-point link directly connects two switches. If the roles of the two ports at the two ends of a point-to-point link meet certain criteria, the two ports can turn to the forwarding state rapidly by exchanging synchronization packets, thus reducing the forward delay.

You can determine whether or not the link connected to a port is a point-to-point link in one of the following two ways.

Setting the Link Type of a Port to P2P in system view

Follow these steps to specify whether the link connected to a port is point-to-point link in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Specify whether the link connected to a port is point-to-point link	**stp interface** *interface-list* **point-to-point** { **force-true** | **force-false** | **auto** }	Required The **auto** keyword is adopted by default.

Setting the Link Type of a Port to P2P in Ethernet port view

Follow these steps to specify whether the link connected to a port is point-to-point link in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

To do...	Use the command...	Remarks
Specify whether the link connected to a port is a point-to-point link	**stp point-to-point** { **force-true** | **force-false** | **auto** }	Required The **auto** keyword is adopted by default.

Note

- If you configure the link connected to a port in an aggregation group as a point-to-point link, the configuration will be synchronized to the rest ports in the same aggregation group.
- If an auto-negotiating port operates in full duplex mode after negotiation, you can configure the link of the port as a point-to-point link.

After you configure the link of a port as a point-to-point link, the configuration applies to all the MSTIs the port belongs to. If the actual physical link of a port is not a point-to-point link and you forcibly configure the link as a point-to-point link, loops may occur temporarily.

Configuration example

Configure the link connected to Ethernet 1/0/1 as a point-to-point link.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface Ethernet 1/0/1 point-to-point force-true
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp point-to-point force-true
```

Enabling MSTP

Configuration procedure

Follow these steps to enable MSTP in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable MSTP	**stp enable**	Required MSTP is enabled globally by default.
Disable MSTP on specified ports	**stp interface** *interface-list* **disable**	Optional By default, MSTP is enabled on all ports. To enable a switch to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree calculation, this operation saves CPU resources of the switch.

Follow these steps to enable MSTP in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable MSTP	**stp enable**	Required MSTP is enabled globally by default.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Disable MSTP on the port	**stp disable**	Optional By default, MSTP is enabled on all ports. To enable a switch to operate more flexibly, you can disable MSTP on specific ports. As MSTP-disabled ports do not participate in spanning tree calculation, this operation saves CPU resources of the switch.

Other MSTP-related settings can take effect only after MSTP is enabled on the switch.

Configuration example

Disable MSTP on Ethernet 1/0/1.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface Ethernet 1/0/1 disable
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp disable
```

Configuring Leaf Nodes

Configuring the MST Region

Refer to Configuring an MST Region.

Configuring How a Port Recognizes and Sends MSTP Packets

Refer to Configuring How a Port Recognizes and Sends MSTP Packets.

Configuring the Timeout Time Factor

Refer to Configuring the Timeout Time Factor.

Configuring the Maximum Transmitting Rate on the Current Port

Refer to Configuring the Maximum Transmitting Rate on the Current Port.

Configuring a Port as an Edge Port

Refer to Configuring the Current Port as an Edge Port.

Configuring the Path Cost for a Port

The path cost parameter reflects the rate of the link connected to the port. For a port on an MSTP-enabled switch, the path cost may be different in different MSTIs. You can enable flows of different VLANs to travel along different physical links by configuring appropriate path costs on ports, so that VLAN-based load balancing can be implemented.

Path cost of a port can be determined by the switch or through manual configuration.

Standards for calculating path costs of ports

Currently, a switch can calculate the path costs of ports based on one of the following standards:

- **dot1d-1998**: Adopts the IEEE 802.1D-1998 standard to calculate the default path costs of ports.
- **dot1t**: Adopts the IEEE 802.1t standard to calculate the default path costs of ports.

Follow these steps to specify the standard for calculating path costs:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Specify the standard for calculating the default path costs of the links connected to the ports of the switch	**stp pathcost-standard** { **dot1d-1998** | **dot1t** }	Optional By default, the dot1t standard is used to calculate the default path costs of ports.

Table 1-7 Transmission rates vs. path costs

Rate	Operation mode (half-/full-duplex)	802.1D-1998	IEEE 802.1t
0	—	65,535	200,000,000
10 Mbps	Half-duplex/Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	100 95 95 95	2,000,000 1,000,000 666,666 500,000
100 Mbps	Half-duplex/Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	19 15 15 15	200,000 100,000 66,666 50,000
1,000 Mbps	Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	4 3 3 3	20,000 10,000 6,666 5,000
10 Gbps	Full-duplex Aggregated link 2 ports Aggregated link 3 ports Aggregated link 4 ports	2 1 1 1	2,000 1,000 666 500

Normally, the path cost of a port operating in full-duplex mode is slightly less than that of the port operating in half-duplex mode.

When calculating the path cost of an aggregated link, the 802.1D-1998 standard does not take the number of the ports on the aggregated link into account, whereas the 802.1T standard does. The following formula is used to calculate the path cost of an aggregated link:

Path cost = 200,000,000 / link transmission rate

Where, “link transmission rate” is the sum of the rates of all the unblocked ports on the aggregated link measured in 100 Kbps.

Configure the path cost for specific ports

Follow these steps to configure the path cost for specified ports in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the path cost for specified ports	**stp interface** *interface-list* [**instance** *instance-id*] **cost** *cost*	Required An MSTP-enabled switch can calculate path costs for all its ports automatically.

Follow these steps to configure the path cost for a port in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the path cost for the port	**stp** [**instance** *instance-id*] **cost** *cost*	Required An MSTP-enabled switch can calculate path costs for all its ports automatically.

Changing the path cost of a port may change the role of the port and put it in state transition. Executing the **stp cost** command with the *instance-id* argument being 0 sets the path cost on the CIST for the port.

Configuration example (A)

Configure the path cost of Ethernet 1/0/1 in MSTI 1 to be 2,000.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface Ethernet 1/0/1 instance 1 cost 2000
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp instance 1 cost 2000
```

Configuration example (B)

Configure the path cost of Ethernet 1/0/1 in MSTI 1 to be calculated by the MSTP-enabled switch according to the IEEE 802.1D-1998 standard.

1) Perform this configuration in system view

```
<Sysname> system-view
```

```
[Sysname] undo stp interface Ethernet 1/0/1 instance 1 cost
[Sysname] stp pathcost-standard dot1d-1998
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] undo stp instance 1 cost
[Sysname-Ethernet1/0/1] quit
[Sysname] stp pathcost-standard dot1d-1998
```

Configuring Port Priority

Port priority is an important criterion on determining the root port. In the same condition, the port with the smallest port priority value becomes the root port.

A port on an MSTP-enabled switch can have different port priorities and play different roles in different MSTIs. This enables packets of different VLANs to be forwarded along different physical paths, so that VLAN-based load balancing can be implemented.

You can configure port priority in one of the following two ways.

Configure port priority in system view

Follow these steps to configure port priority in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure port priority for specified ports	**stp interface** *interface-list* **instance** *instance-id* **port priority** *priority*	Required The default port priority is 128.

Configure port priority in Ethernet port view

Follow these steps to configure port priority in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure port priority for the port	**stp** [**instance** *instance-id*] **port priority** *priority*	Required. The default port priority is 128.

Changing port priority of a port may change the role of the port and put the port into state transition.

A smaller port priority value indicates a higher possibility for the port to become the root port. If all the ports of a switch have the same port priority value, the port priorities are determined by the port indexes. Changing the priority of a port will cause spanning tree recalculation.

You can configure port priorities according to actual networking requirements.

Configuration example

Configure the port priority of Ethernet 1/0/1 in MSTI 1 to be 16.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface Ethernet 1/0/1 instance 1 port priority 16
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp instance 1 port priority 16
```

Setting the Link Type of a Port to P2P

Refer to Setting the Link Type of a Port to P2P.

Enabling MSTP

Refer to Enabling MSTP.

Performing mCheck Operation

Ports on an MSTP-enabled switch can operate in three modes: STP-compatible, RSTP-compatible, and MSTP.

If a port on a device running MSTP (or RSTP) connects to a device running STP, this port will automatically migrate to the STP-compatible mode. However, it will not be able to migrate automatically back to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode under the following circumstances:

- The device running STP is shut down or removed.
- The device running STP migrates to the MSTP (or RSTP) mode.

By then, you can perform an mCheck operation to force the port to migrate to the MSTP (or RSTP) mode.

Configuration Prerequisites

MSTP runs normally on the switch.

Configuration Procedure

You can perform the mCheck operation in the following two ways.

Perform the mCheck operation in system view

Follow these steps to perform the mCheck operation in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Perform the mCheck operation	**stp** [**interface** *interface-list*] **mcheck**	Required

Perform the mCheck operation in Ethernet port view

Follow these steps to perform the mCheck operation in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Perform the mCheck operation	**stp mcheck**	Required

Configuration Example

Perform the mCheck operation on Ethernet 1/0/1.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface Ethernet 1/0/1 mcheck
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp mcheck
```

Configuring Guard Functions

The following guard functions are available on an MSTP-enabled switch: BPDU guard, root guard, loop guard, and TC-BPDU attack guard.

Configuring BPDU Guard

Normally, the access ports of the devices operating on the access layer are directly connected to terminals (such as PCs) or file servers. These ports are usually configured as edge ports to achieve rapid transition. But they resume non-edge ports automatically upon receiving configuration BPDUs, which causes spanning tree recalculation and network topology jitter.

Normally, no configuration BPDU will reach edge ports. But malicious users can attack a network by sending configuration BPDUs deliberately to edge ports to cause network jitter. You can prevent this type of attacks by utilizing the BPDU guard function. With this function enabled on a switch, the switch shuts down the edge ports that receive configuration BPDUs and then reports these cases to the administrator. Ports shut down in this way can only be restored by the administrator.

Note

You are recommended to enable BPDU guard for devices with edge ports configured.

Configuration Prerequisites

MSTP runs normally on the switch.

Configuration procedure

Follow these steps to configure BPDU guard:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable the BPDU guard function	**stp bpdu-protection**	Required The BPDU guard function is disabled by default.

Configuration example

Enable the BPDU guard function.

```
<Sysname> system-view
[Sysname] stp bpdu-protection
```

Caution

As Gigabit ports of a 3Com switch 4500 cannot be shut down, the BPDU guard function is not applicable to these ports even if you enable the BPDU guard function and specify these ports to be MSTP edge ports.

Configuring Root Guard

A root bridge and its secondary root bridges must reside in the same region. The root bridge of the CIST and its secondary root bridges are usually located in the high-bandwidth core region. Configuration errors or attacks may result in configuration BPDUs with their priorities higher than that of a root bridge, which causes a new root bridge to be elected and network topology jitter to occur. In this case, flows that should travel along high-speed links may be led to low-speed links, and network congestion may occur.

You can avoid this problem by utilizing the root guard function. Ports with this function enabled can only be kept as designated ports in all MSTIs. When a port of this type receives configuration BPDUs with higher priorities, it turns to the discarding state (rather than become a non-designated port) and stops forwarding packets (as if it is disconnected from the link). It resumes the normal state if it does not receive any configuration BPDUs with higher priorities for a specified period.

Note

- You are recommended to enable root guard on the designated ports of a root bridge.
- Loop guard, root guard, and edge port settings are mutually exclusive. With one of these functions enabled on a port, any of the other two functions cannot take effect even if you have configured it on the port.

Configuration Prerequisites

MSTP runs normally on the switch.

Configuration procedure

Follow these steps to configure the root guard function in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable the root guard function on specified ports	**stp interface** *interface-list* **root-protection**	Required The root guard function is disabled by default.

Follow these steps to enable the root guard function in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**Interface** *interface-type interface-number*	—
Enable the root guard function on the current port	**stp root-protection**	Required The root guard function is disabled by default.

Configuration example

Enable the root guard function on Ethernet 1/0/1.

1) Perform this configuration in system view

```
<Sysname> system-view
[Sysname] stp interface Ethernet 1/0/1 root-protection
```

2) Perform this configuration in Ethernet port view

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp root-protection
```

Configuring Loop Guard

A switch maintains the states of the root port and other blocked ports by receiving and processing BPDUs from the upstream switch. These BPDUs may get lost because of network congestions or unidirectional link failures. If a switch does not receive BPDUs from the upstream switch for certain period, the switch selects a new root port; the original root port becomes a designated port; and the blocked ports turns to the forwarding state. This may cause loops in the network.

The loop guard function suppresses loops. With this function enabled, if link congestions or unidirectional link failures occur, both the root port and the blocked ports become designated ports and turn to the discarding state. In this case, they stop forwarding packets, and thereby loops can be prevented.

Note

- You are recommended to enable loop guard on the root port and alternate port of a non-root bridge.
- Loop guard, root guard, and edge port settings are mutually exclusive. With one of these functions enabled on a port, any of the other two functions cannot take effect even if you have configured it on the port.

Configuration Prerequisites

MSTP runs normally on the switch.

Configuration procedure

Follow these steps to configure loop guard:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the loop guard function on the current port	**stp loop-protection**	Required The loop guard function is disabled by default.

Configuration example

Enable the loop guard function on Ethernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] stp loop-protection
```

Configuring TC-BPDU Attack Guard

Normally, a switch removes its MAC address table and ARP entries upon receiving Topology Change BPDUs (TC-BPDUs). If a malicious user sends a large amount of TC-BPDUs to a switch in a short period, the switch may be busy in removing the MAC address table and ARP entries, which may affect spanning tree calculation, occupy large amount of bandwidth and increase switch CPU utilization.

With the TC-BPDU attack guard function enabled, a switch performs a removing operation upon receiving a TC-BPDU and triggers a timer (set to 10 seconds by default) at the same time. Before the timer expires, the switch only performs the removing operation for limited times (up to six times by default) regardless of the number of the TC-BPDUs it receives. Such a mechanism prevents a switch from being busy in removing the MAC address table and ARP entries.

You can use the **stp tc-protection threshold** command to set the maximum times for a switch to remove the MAC address table and ARP entries in a specific period. When the number of the TC-BPDUs received within a period is less than the maximum times, the switch performs a removing operation upon receiving a TC-BPDU. After the number of the TC-BPDUs received reaches the maximum times, the switch stops performing the removing operation. For example, if you set the

maximum times for a switch to remove the MAC address table and ARP entries to 100 and the switch receives 200 TC-BPDUs in the period, the switch removes the MAC address table and ARP entries for only 100 times within the period.

Configuration prerequisites

MSTP runs normally on the switch.

Configuration procedure

Follow these steps to configure the TC-BPDU attack guard function:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable the TC-BPDU attack guard function	**stp tc-protection enable**	Required The TC-BPDU attack guard function is disabled by default.
Set the maximum times that a switch can remove the MAC address table and ARP entries within each 10 seconds	**stp tc-protection threshold** *number*	Optional

Configuration example

Enable the TC-BPDU attack guard function

```
<Sysname> system-view
[Sysname] stp tc-protection enable
```

Set the maximum times for the switch to remove the MAC address table and ARP entries within 10 seconds to 5.

```
<Sysname> system-view
[Sysname] stp tc-protection threshold 5
```

Configuring Digest Snooping

Introduction

According to IEEE 802.1s, two interconnected switches can communicate with each other through MSTIs in an MST region only when the two switches have the same MST region-related configuration. Interconnected MSTP-enabled switches determine whether or not they are in the same MST region by checking the configuration IDs of the BPDUs between them (A configuration ID contains information such as region ID and configuration digest).

As some other manufacturers' switches adopt proprietary spanning tree protocols, they cannot communicate with the other switches in an MST region even if they are configured with the same MST region-related settings as the other switches in the MST region.

This problem can be overcome by implementing the digest snooping feature. If a port on a 3Com switch 4500 is connected to another manufacturer's switch that has the same MST region-related configuration as its own but adopts a proprietary spanning tree protocol, you can enable digest snooping on the port. Then the switch 4500 regards another manufacturer's switch as in the same region; it records the configuration digests carried in the BPDUs received from another manufacturer's

switch, and put them in the BPDUs to be sent to the another manufacturer's switch. In this way, the switch 4500 can communicate with another manufacturer’s switches in the same MST region.

Caution

The digest snooping function is not applicable to edge ports.

Configuring Digest Snooping

Configure the digest snooping feature on a switch to enable it to communicate with other switches adopting proprietary protocols to calculate configuration digests in the same MST region through MSTIs.

Configuration prerequisites

The switch to be configured is connected to another manufacturer's switch adopting a proprietary spanning tree protocol. MSTP and the network operate normally.

Configuration procedure

Follow these steps to configure digest snooping:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the digest snooping feature	**stp config-digest-snooping**	Required The digest snooping feature is disabled on a port by default.
Return to system view	**quit**	—
Enable the digest snooping feature globally	**stp config-digest-snooping**	Required The digest snooping feature is disabled globally by default.
Display the current configuration	**display current-configuration**	Available in any view

Note

- When the digest snooping feature is enabled on a port, the port state turns to the discarding state. That is, the port will not send BPDU packets. The port is not involved in the STP calculation until it receives BPDU packets from the peer port.
- The digest snooping feature is needed only when your switch is connected to another manufacturer's switches adopting proprietary spanning tree protocols.
- To enable the digest snooping feature successfully, you must first enable it on all the ports of your switch that are connected to another manufacturer's switches adopting proprietary spanning tree protocols and then enable it globally.
- To enable the digest snooping feature, the interconnected switches and another manufacturer's switch adopting proprietary spanning tree protocols must be configured with exactly the same MST region-related configurations (including region name, revision level, and VLAN-to-instance mapping).
- The digest snooping feature must be enabled on all the switch ports that connect to another manufacturer's switches adopting proprietary spanning tree protocols in the same MST region.
- When the digest snooping feature is enabled globally, the VLAN-to-instance mapping table cannot be modified.
- The digest snooping feature is not applicable to boundary ports in an MST region.
- The digest snooping feature is not applicable to edge ports in an MST region.

Configuring Rapid Transition

Introduction

Designated ports of RSTP-enabled or MSTP-enabled switches use the following two types of packets to implement rapid transition:

- Proposal packets: Packets sent by designated ports to request rapid transition
- Agreement packets: Packets used to acknowledge rapid transition requests

Both RSTP and MSTP specify that the upstream switch can perform rapid transition operation on the designated port only when the port receives an agreement packet from the downstream switch. The difference between RSTP and MSTP are:

- For MSTP, the upstream switch sends agreement packets to the downstream switch; and the downstream switch sends agreement packets to the upstream switch only after it receives agreement packets from the upstream switch.
- For RSTP, the upstream switch does not send agreement packets to the downstream switch.

Figure 1-6 and Figure 1-7 illustrate the rapid transition mechanisms on designated ports in RSTP and MSTP.

Figure 1-6 The RSTP rapid transition mechanism

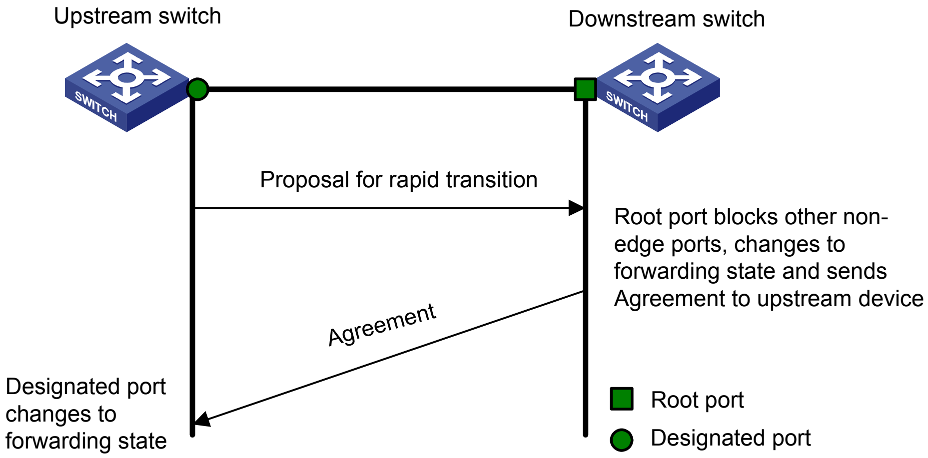
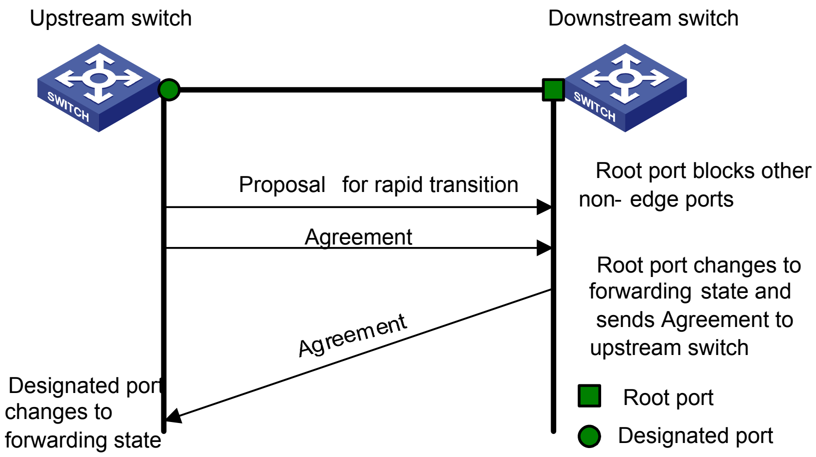


Figure 1-7 The MSTP rapid transition mechanism



The cooperation between MSTP and RSTP is limited in the process of rapid transition. For example, when the upstream switch adopts RSTP, the downstream switch adopts MSTP and the downstream switch does not support RSTP-compatible mode, the root port on the downstream switch receives no agreement packet from the upstream switch and thus sends no agreement packets to the upstream switch. As a result, the designated port of the upstream switch fails to transit rapidly and can only turn to the forwarding state after a period twice the forward delay.

Some other manufacturers' switches adopt proprietary spanning tree protocols that are similar to RSTP in the way to implement rapid transition on designated ports. When a switch of this kind operating as the upstream switch connects with a 3Com switch 4500 running MSTP, the upstream designated port fails to change its state rapidly.

The rapid transition feature is developed to resolve this problem. When a 3Com switch 4500 running MSTP is connected in the upstream direction to another manufacturer's switch running proprietary spanning tree protocols, you can enable the rapid transition feature on the ports of the switch 4500 operating as the downstream switch. Among these ports, those operating as the root ports will then send agreement packets to their upstream ports after they receive proposal packets from the upstream designated ports, instead of waiting for agreement packets from the upstream switch. This enables designated ports of the upstream switch to change their states rapidly.

Configuring Rapid Transition

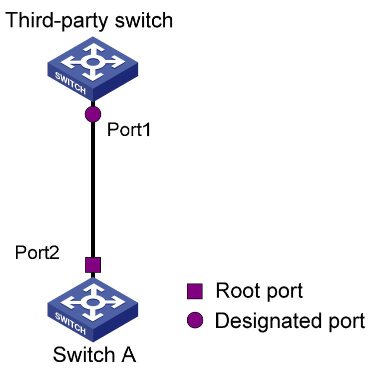
Configuration prerequisites

As shown in Figure 1-8, a 3Com switch 4500 is connected to another manufacturer's switch. The former operates as the downstream switch, and the latter operates as the upstream switch. The network operates normally.

The upstream switch is running a proprietary spanning tree protocol that is similar to RSTP in the way to implement rapid transition on designated ports. Port 1 is the designated port.

The downstream switch is running MSTP. Port 2 is the root port.

Figure 1-8 Network diagram for rapid transition configuration



Configuration procedure

1) Configure the rapid transition feature in system view

Follow these steps to configure the rapid transition feature in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable the rapid transition feature	**stp interface** *interface-type interface-number* **no-agreement-check**	Required By default, the rapid transition feature is disabled on a port.

2) Configure the rapid transition feature in Ethernet port view

Follow these steps to configure the rapid transition feature in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the rapid transition feature	**stp no-agreement-check**	Required By default, the rapid transition feature is disabled on a port.

Note

- The rapid transition feature can be enabled on only root ports or alternate ports.
- If you configure the rapid transition feature on a designated port, the feature does not take effect on the port.

MSTP Maintenance Configuration

Introduction

In a large-scale network with MSTP enabled, there may be many MSTP instances, and so the status of a port may change frequently. In this case, maintenance personnel may expect that log/trap information is output to the log host when particular ports fail, so that they can check the status changes of those ports through alarm information.

Enabling Log/Trap Output for Ports of MSTP Instance

Follow these steps to enable log/trap output for ports of MSTP instance:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable log/trap output for the ports of a specified instance	**stp** [**instance** *instance-id*] **portlog**	Required By default, log/trap output is disabled for the ports of all instances.
Enable log/trap output for the ports of all instances	**stp portlog all**	Required By default, log/trap output is disabled for the ports of all instances.

Configuration Example

Enable log/trap output for the ports of instance 1.

```
<Sysname> system-view
[Sysname] stp instance 1 portlog
```

Enable log/trap output for the ports of all instances.

```
<Sysname> system-view
[Sysname] stp portlog all
```

Enabling Trap Messages Conforming to 802.1d Standard

A switch sends trap messages conforming to 802.1d standard to the network management device in the following two cases:

- The switch becomes the root bridge of an instance.
- Network topology changes are detected.

Configuration procedure

Follow these steps to enable trap messages conforming to 802.1d standard:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable trap messages conforming to 802.1d standard in an instance	**stp** [**instance** *instance-id*] **dot1d-trap** [**newroot** | **topologychange**] **enable**	Required

Configuration example

Enable a switch to send trap messages conforming to 802.1d standard to the network management device when the switch becomes the root bridge of instance 1.

```
<Sysname> system-view
[Sysname] stp instance 1 dot1d-trap newroot enable
```

Displaying and Maintaining MSTP

To do...	Use the command...	Remarks
Display the state and statistics information about spanning trees of the current device	**display stp** [**instance** *instance-id*] [**interface** *interface-list* | **slot** *slot-number*] [**brief**]	Available in any view
Display region configuration	**display stp region-configuration**	
Display information about the ports that are shut down by STP protection	**display stp portdown**	
Display information about the ports that are blocked by STP protection	**display stp abnormalport**	
Display information about the root port of the instance where the switch reside	**display stp root**	
Clear statistics about MSTP	**reset stp** [**interface** *interface-list*]	Available in user view

MSTP Configuration Example

Network requirements

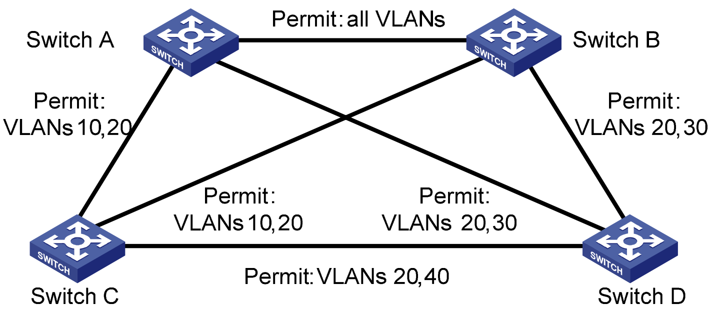
Implement MSTP in the network shown in Figure 1-9 to enable packets of different VLANs to be forwarded along different MSTIs. The detailed configurations are as follows:

- All switches in the network belong to the same MST region.
- Packets of VLAN 10, VLAN 30, VLAN 40, and VLAN 20 are forwarded along MSTI 1, MSTI 3, MSTI 4, and MSTI 0 respectively.

In this network, Switch A and Switch B operate on the convergence layer; Switch C and Switch D operate on the access layer. VLAN 10 and VLAN 30 are limited in the convergence layer and VLAN 40 is limited in the access layer. Switch A and Switch B are configured as the root bridges of MSTI 1 and MSTI 3 respectively. Switch C is configured as the root bridge of MSTI 4.

Network diagram

Figure 1-9 Network diagram for MSTP configuration



Note

The word "permit" shown in Figure 1-9 means the corresponding link permits packets of specific VLANs.

Configuration procedure

1) Configure Switch A

Enter MST region view.

```
<Sysname> system-view
[Sysname] stp region-configuration
```

Configure the region name, VLAN-to-instance mapping table, and revision level for the MST region.

```
[Sysname-mst-region] region-name example
[Sysname-mst-region] instance 1 vlan 10
[Sysname-mst-region] instance 3 vlan 30
[Sysname-mst-region] instance 4 vlan 40
[Sysname-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[Sysname-mst-region] active region-configuration
```

Specify Switch A as the root bridge of MSTI 1.

```
[Sysname] stp instance 1 root primary
```

2) Configure Switch B

Enter MST region view.

```
<Sysname> system-view
[Sysname] stp region-configuration
```

Configure the region name, VLAN-to-instance mapping table, and revision level for the MST region.

```
[Sysname-mst-region] region-name example
[Sysname-mst-region] instance 1 vlan 10
[Sysname-mst-region] instance 3 vlan 30
[Sysname-mst-region] instance 4 vlan 40
[Sysname-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[Sysname-mst-region] active region-configuration
```

Specify Switch B as the root bridge of MSTI 3.

```
[Sysname] stp instance 3 root primary
```

3) Configure Switch C.

Enter MST region view.

```
<Sysname> system-view
[Sysname] stp region-configuration
```

Configure the MST region.

```
[Sysname-mst-region] region-name example
[Sysname-mst-region] instance 1 vlan 10
[Sysname-mst-region] instance 3 vlan 30
[Sysname-mst-region] instance 4 vlan 40
[Sysname-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[Sysname-mst-region] active region-configuration
```

Specify Switch C as the root bridge of MSTI 4.

```
[Sysname] stp instance 4 root primary
```

4) Configure Switch D

Enter MST region view.

```
<Sysname> system-view
[Sysname] stp region-configuration
```

Configure the MST region.

```
[Sysname-mst-region] region-name example
[Sysname-mst-region] instance 1 vlan 10
[Sysname-mst-region] instance 3 vlan 30
[Sysname-mst-region] instance 4 vlan 40
[Sysname-mst-region] revision-level 0
```

Activate the settings of the MST region manually.

```
[Sysname-mst-region] active region-configuration
```

Table of Contents

1 IP Routing Protocol Overview

Go to these sections for information you are interested in:

Introduction to IP Route and Routing Table

IP Route

Routers are used for route selection on the Internet. As a router receives a packet, it selects an appropriate route (through a network) according to the destination address of the packet and forwards the packet to the next router. The last router on the route is responsible for delivering the packet to the destination host.

Routing Table

Function

The key for a router to forward packets is the routing table. Each router maintains a routing table. Each entry in this table contains an IP address that represents a host/subnet and specifies which physical port on the router should be used to forward the packets destined for the host/subnet. And the router forwards those packets through this port to the next router or directly to the destination host if the host is on a network directly connected to the router.

Routes in a routing table can be divided into three categories by origin:

- Direct routes: Routes discovered by data link protocols, also known as interface routes.
- Static routes: Routes that are manually configured.
- Dynamic routes: Routes that are discovered dynamically by routing protocols.

Routing entry

Each routing entry in a routing table contains:

- Destination: It identifies the address of the destination host or network of an IP packet.
- Mask: Along with the destination address, it identifies the address of the network segment where the destination host or router resides. By performing a logical AND operation between destination address and network mask, you can get the address of the network segment where the destination host or router resides. For example, if the destination address is 129.102.8.10 and the mask is 255.255.0.0, the address of the network segment where the destination host or router resides is 129.102.0.0. A mask consists of some consecutive 1s, represented either in dotted decimal notation or by the number of the consecutive 1s in the mask.
- Interface: It indicates through which interface IP packets should be forwarded to the destination.
- Nexthop: It indicates the next router that IP packets will pass through to reach the destination.

- Preference: There may be multiple routes with different next hops to the same destination. These routes may be discovered by different routing protocols, or be manually configured static routes. The one with the highest preference (the smallest numerical value) will be selected as the current optimal route.

According to different destinations, routes fall into the following categories:

- Subnet route: The destination is a subnet.
- Host route: The destination is a host.

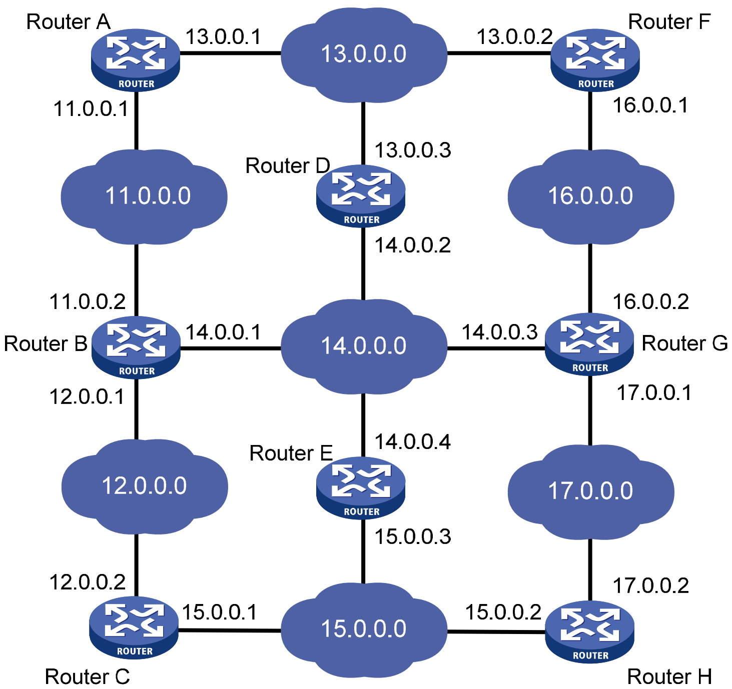
In addition, according to whether the network where the destination resides is directly connected to the router, routes fall into the following categories:

- Direct route: The router is directly connected to the network where the destination resides.
- Indirect route: The router is not directly connected to the network where the destination resides.

In order to avoid an oversized routing table, you can set a default route. All the packets for which the router fails to find a matching entry in the routing table will be forwarded through this default route.

Figure 1-1shows a relatively complicated internet environment, the number in each network cloud indicate the network address. Router G is connected to three networks, and so it has three IP addresses and three physical ports. Its routing table is shown in Figure 1-1.

Figure 1-1 Routing table



Destination Network	Nexthop	Interface
11.0.0.0	14.0.0.1	3
12.0.0.0	14.0.0.1	3
13.0.0.0	16.0.0.1	2
14.0.0.0	14.0.0.3	3
15.0.0.0	17.0.0.2	1
16.0.0.0	16.0.0.2	2
17.0.0.0	17.0.0.1	1

Routing Protocol Overview

Static Routing and Dynamic Routing

Static routing is easy to configure and requires less system resources. It works well in small, stable networks with simple topologies. It cannot adapt itself to any network topology change automatically so that you must perform routing configuration again whenever the network topology changes.

Dynamic routing is based on dynamic routing protocols, which can detect network topology changes and recalculate the routes accordingly. Therefore, dynamic routing is suitable for large networks. It is complicated to configure, and it not only imposes higher requirements on the system than static routing, but also occupies a certain amount of network resources.

Classification of Dynamic Routing Protocols

Dynamic routing protocols can be classified based on the following standards:

Operational scope

- Interior Gateway Protocols (IGPs): Work within an autonomous system, typically including RIP, OSPF, and IS-IS.
- Exterior Gateway Protocols (EGPs): Work between autonomous systems. The most popular one is BGP.

Note

An autonomous system refers to a group of routers that share the same route policy and work under the same administration.

Routing algorithm

- Distance-vector protocols: RIP and BGP. BGP is also considered a path-vector protocol.
- Link-state protocols: OSPF and IS-IS.

The main differences between the above two types of routing algorithms lie in the way routes are discovered and calculated.

Type of the destination address

- Unicast routing protocols: RIP, OSPF, BGP, and IS-IS.
- Multicast routing protocols: PIM-SM and PIM-DM.

This chapter focuses on unicast routing protocols. For information on multicast routing protocols, refer to the part discussing *Multicast*.

Routing Protocols and Routing Priority

Different routing protocols may find different routes (including static routes) to the same destination. However, not all of those routes are optimal. In fact, at a particular moment, only one protocol can uniquely determine the current optimal routing to the destination. For the purpose of route selection,

each routing protocol (including static routes) is assigned a priority. The route found by the routing protocol with the highest priority is preferred.

The following table lists some routing protocols and the default priorities for routes found by them:

Table 1-1 Routing protocols and priorities of their default route

Routing approach	Priority
DIRECT	0
OSPF	10
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
UNKNOWN	255

Note

- The smaller the priority value, the higher the priority.
- The priority for a direct route is always 0, which you cannot change. Any other type of routes can have their priorities manually configured.
- Each static route can be configured with a different priority.

Load Sharing and Route Backup

Load sharing

A given routing protocol may find several routes with the same metric to the same destination, and if this protocol has the highest priority among all the active protocols, these routes will be considered valid and are used to forward packets, thus achieving load sharing.

Route backup

You can configure multiple routes to the same destination, expecting the one with the highest priority to be the primary route and all the rest backup routes.

Route backup can help improve network reliability. Automatic switching can happen between the primary route and a backup route.

Under normal circumstances, packets are forwarded through the primary route. When the primary route goes down, the route with the highest priority among the backup routes is selected to forward packets. When the primary route recovers, the route selection process is performed again and the primary route is selected again to forward packets.

Routing Information Sharing

As different routing protocols use different algorithms to calculate routes, they may discover different routes. In a large network with multiple routing protocols, it is required for routing protocols to share their

routing information. Each routing protocol shares routing information discovered by other routing protocols through a route redistribution mechanism.

Displaying and Maintaining a Routing Table

To do…	Use the command…	Remarks
Display brief information about a routing table	**display ip routing-table** [**|** { **begin | exclude | include** } *regular-expression*]	Available in any view
Display detailed information about a routing table	**display ip routing-table verbose**	
Display information about routes permitted by a basic ACL	**display ip routing-table acl** *acl-number* [**verbose**]	
Display information about routes permitted by a prefix list	**display ip routing-table ip-prefix** *ip-prefix-name* [**verbose**]	
Display routes to a specified destination	**display ip routing-table** *ip-address* [*mask* | *mask-length*] [**longer-match**] [**verbose**]	
Display routes to specified destinations	**display ip routing-table** *ip-address1* { *mask1* | *mask-length1* } *ip-address2* { *mask2* | *mask-length2* } [**verbose**]	
Display routes discovered by a routing protocol	**display ip routing-table protocol** *protocol* [**inactive** | **verbose**]	
Display the tree-structured routing table information	**display ip routing-table radix**	
Display statistics about a routing table	**display ip routing-table statistics**	
Clear statistics about a routing table	**reset ip routing-table statistics protocol** { **all** | *protocol* }	Available in user view

2 Static Route Configuration

When configuring a static route, go to these sections for information you are interested in:

- Introduction to Static Route
- Static Route Configuration
- Displaying and Maintaining Static Routes
- Static Route Configuration Example
- Troubleshooting a Static Route

Note

The term **router** in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

Introduction to Static Route

Static Route

Static routes are special routes. They are manually configured by the administrator. In a relatively simple network, you only need to configure static routes to make routers work normally. Proper configuration and usage of static routes can improve network performance and ensure sufficient bandwidth for important applications.

When the network topology changes, static routes may become unreachable because they cannot adapt themselves to the change automatically, thus resulting in network interruption. In this case, the network administrator needs to modify the configuration of static routes manually.

Static routes are divided into three types:

- Reachable route: normal route. If a static route to a destination is of this type, the IP packets destined for this destination will be forwarded to the next hop. It is the most common type of static routes.
- Unreachable route: route with the **reject** attribute. If a static route to a destination has the **reject** attribute, all the IP packets destined for this destination will be discarded, and the source hosts will be informed of the unreachability of the destination.
- Blackhole route: route with **blackhole** attribute. If a static route destined for a destination has the **blackhole** attribute, the outgoing interface of this route is the Null 0 interface regardless of the next hop address, and all the IP packets addressed to this destination will be dropped without notifying the source hosts.

The attributes **reject** and **blackhole** are usually used to limit the range of the destinations this router can reach, and help troubleshoot the network.

Default Route

To avoid too large a routing table, you can configure a default route.

When the destination address of a packet fails to match any entry in the routing table,

- If there is default route in the routing table, the default route will be selected to forward the packet.
- If there is no default route, the packet will be discarded and an ICMP Destination Unreachable or Network Unreachable packet will be returned to the source.

A default route can be manually configured or generated by some dynamic routing protocols, such as OSPF and RIP.

Static Route Configuration

Configuration Prerequisites

Before configuring a static route, perform the following tasks:

- Configuring the physical parameters of related interfaces
- Configuring IP addresses for related interfaces

Configuring a Static Route

Follow these steps to configure a static route:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *next-hop* } [**preference** *preference-value*] [**reject** | **blackhole**] [**detect-group** *group number*] [**description** *text*]	Required By default, the system can obtain the route to the subnet directly connected to the router.

Note

- Use the **ip route-static** command to configure a default route by setting the destination IP address and the mask to 0.0.0.0.
- Avoid configuring the next hop address of a static route to the address of an interface on the local switch.
- Different preferences can be configured to implement flexible route management policies.
- For automatic detection information, refer to the part discussing *Auto Detect*.

Displaying and Maintaining Static Routes

To do...	Use the command...	Remarks
Display the current configuration information	**display current-configuration**	Available in any view

To do...	Use the command...	Remarks
Display the brief information of a routing table	**display ip routing-table**	
Display the detailed information of a routing table	**display ip routing-table verbose**	
Display the information of static routes	**display ip routing-table protocol static** [**inactive** | **verbose**]	
Delete all static routes	**delete static-routes all**	Available in system view

Static Route Configuration Example

Network requirements

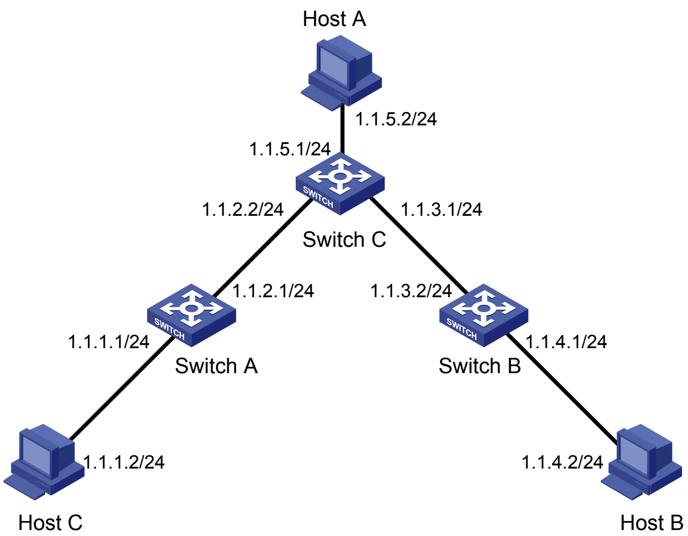
A small company requires that any two nodes in its office network communicate with each other, and that the network structure be simple and stable. The company hopes that the existing devices that do not support any dynamic routing protocol can be fully utilized.

In this case, static routes can implement communication between any two nodes.

Network diagram

According to the network requirements, the network topology is designed as shown in Figure 2-1.

Figure 2-1 Network diagram for static route configuration



Configuration procedure

Note

When only one interface of the device is interconnected with another network segment, you can implement network communication by configuring either a static route or default route.

1) Perform the following configurations on the switch.

Approach 1: Configure static routes on Switch A.

```
<SwitchA> system-view
[SwitchA] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[SwitchA] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

Approach 2: Configure a static route on Switch A.

```
<SwitchA> system-view
[SwitchA] ip route-static 0.0.0.0 0.0.0.0 1.1.2.2
```

Approach 1: Configure static routes on Switch B.

```
<SwitchB> system-view
[SwitchB] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[SwitchB] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

Approach 2: Configure a static route on Switch B.

```
<SwitchB> system-view
[SwitchB] ip route-static 0.0.0.0 0.0.0.0 1.1.3.1
```

Configure static routes on Switch C.

```
<SwitchC> system-view
[SwitchC] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[SwitchC] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

2) Perform the following configurations on the host.

Set the default gateway address of Host A to 1.1.5.1. Detailed configuration procedure is omitted.

Set the default gateway address of Host B to 1.1.4.1. Detailed configuration procedure is omitted.

Set the default gateway address of Host C to 1.1.1.1. Detailed configuration procedure is omitted.

Now, all the hosts and switches in the figure can communicate with each other.

Troubleshooting a Static Route

Symptom: The switch is not configured with a dynamic routing protocol. Both the physical status and the link layer protocol status of an interface are UP, but IP packets cannot be forwarded on the interface.

Solution: Perform the following procedure.

1) Use the **display ip routing-table protocol static** command to view whether the corresponding static route is correctly configured.
2) Use the **display ip routing-table** command to view whether the static route is valid.

3 RIP Configuration

When configuring RIP, go to these sections for information you are interested in:

- RIP Overview
- RIP Configuration Task List
- RIP Configuration Example
- Troubleshooting RIP Configuration

Note

The term **router** in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

RIP Overview

Routing information protocol (RIP) is a simple interior gateway protocol (IGP) suitable for small-sized networks. RIP is not recommended in complicated large networks.

Basic Concepts

RIP

RIP is a distance-vector (D-V) algorithm–based protocol. It uses port 520 to exchange routing information through UDP packets.

RIP uses hop count (also called routing cost) to measure the distance to a destination address. In RIP, the hop count from a router to its directly connected network is 0, and that to a network which can be reached through another router is 1, and so on. To restrict the time to converge, RIP prescribes that the cost is an integer ranging from 0 and 15. The hop count equal to or exceeding 16 is defined as infinite; that is, the destination network or host is unreachable. This limitation makes RIP not suitable for large networks.

To improve performance and avoid routing loop, RIP supports split horizon. Besides, RIP can import routes discovered by other routing protocols.

RIP routing database

Each RIP router has a routing table containing routing entries of all reachable destinations, and each routing entry contains:

- Destination address: IP address of a host or network.
- Next hop: IP address of an interface on the adjacent router that IP packets should pass through to reach the destination.

- Interface: Outbound interface on this router, through which IP packets should be forwarded to reach the destination.
- Metric: Cost from the local router to the destination.
- Route time: Time elapsed since the routing entry was last updated. The time is reset to 0 every time the routing entry is updated.

RIP timers

As defined in RFC 1058, RIP is controlled by three timers: Period update, Timeout, and Garbage-collection.

- Period update timer: The period update timer defines the interval between routing updates.
- Timeout timer: The timeout timer defines the route aging time. If no update for a route is received after the aging time elapses, the metric of the route is set to 16 in the routing table.
- Garbage-collection timer: The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.

Routing loops prevention

RIP is a distance-vector (D-V) based routing protocol. Since a RIP router advertises its own routing table to neighbors, routing loops may occur.

RIP uses the following mechanisms to prevent routing loops.

- Counting to infinity. The metric value of 16 is defined as unreachable. When a routing loop occurs, the metric value of the route will increment to 16.
- Split horizon. A router does not send the routing information learned from a neighbor back to the neighbor to prevent routing loops and save the bandwidth.

RIP Startup and Operation

The whole process of RIP startup and operation is as follows:

- Once RIP is enabled on a router, the router broadcasts or multicasts a request packet to its neighbors. Upon receiving the packet, each neighbor running RIP answers a response packet containing its routing table information.
- When this router receives a response packet, it updates its local routing table and sends a triggered update packet to the neighbors. Upon receiving the triggered update packet, the neighbor sends the packet to all its neighbors. After a series of update triggering processes, each router can get and keep the updated routing information.
- By default, RIP sends its routing table to its neighbors every 30 seconds. Upon receiving the packets, the neighbors maintain their own routing tables and select optimal routes, and then advertise update information to their respective neighbors so as to make the updated routes known globally. Furthermore, RIP uses the aging mechanism to handle the timeout routes to ensure real-time and valid routes.

RIP Configuration Task List

Complete the following tasks to configure RIP:

Task		Remarks
Configuring Basic RIP Functions	Enabling RIP on the interfaces attached to a specified network segment	Required
	Setting the RIP operating status on an interface	Optional
	Specifying the RIP version on an interface	Optional
Configuring RIP Route Control	Setting the additional routing metrics of an interface	Optional
	Configuring RIP route summarization	Optional
	Disabling the router from receiving host routes	Optional
	Configuring RIP to filter incoming/outgoing routes	Optional
	Setting RIP preference	Optional
	Enabling load sharing among RIP interfaces	Optional
	Configuring RIP to redistribute routes from another protocol	Optional
RIP Network Adjustment and Optimization	Configuring RIP timers	Optional
	Configuring split horizon	Optional
	Configuring RIP-1 packet zero field check	Optional
	Setting RIP-2 packet authentication mode	Optional
	Configuring RIP to unicast RIP packets	Optional

Basic RIP Configuration

Configuration Prerequisites

Before configuring basic RIP functions, perform the following tasks:

- Configuring the link layer protocol
- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer

Configuring Basic RIP Functions

Enabling RIP on the interfaces attached to a specified network segment

Follow these steps to enable RIP on the interfaces attached to a specified network segment:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable RIP and enter RIP view	**rip**	Required
Enable RIP on the specified interface	**network** *network-address*	Required Disabled by default

Note

- Related RIP commands configured in interface view can take effect only after RIP is enabled.
- RIP operates on the interfaces attached to a specified network segment. When RIP is disabled on an interface, it does not operate on the interface, that is, it neither receives/sends routes on the interface, nor forwards any interface route. Therefore, after RIP is enabled globally, you must also specify its operating network segments to enable it on the corresponding interfaces.

Setting the RIP operating status on an interface

Follow these steps to set the RIP operating status on an interface:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Enable the interface to receive RIP update packets	**rip input**	Optional Enabled by default
Enable the interface to send RIP update packets	**rip output**	
Enable the interface to receive and send RIP update packets	**rip work**	

Specifying the RIP version on an interface

Follow these steps to specify the RIP version on an interface:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Specify the version of the RIP running on the interface	**rip version** { **1** | **2** [**broadcast** | **multicast**] }	Optional By default, the version of the RIP running on an interface is RIP-1.

RIP Route Control

In actual implementation, it may be needed to control RIP routing information more accurately to accommodate complex network environments. By performing the configuration described in the following sections, you can:

- Control route selection by adjusting additional routing metrics on interfaces running RIP.
- Reduce the size of the routing table by setting route summarization and disabling the receiving of host routes.
- Filter incoming and outgoing routes.

- Set the preference of RIP to change the preference order of routing protocols. This order makes sense when more than one route to the same destination is discovered by multiple routing protocols.
- Redistribute external routes in an environment with multiple routing protocols.

Configuration Prerequisites

Before configuring RIP route control, perform the following tasks:

- Configuring network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

Configuring RIP Route Control

Setting the additional routing metrics of an interface

Additional metric is the metric added to the original metrics of RIP routes on an interface. It does not directly change the metric value of a RIP route in the routing table of a router, but will be added to incoming or outgoing RIP routes on the interface.

Follow these steps to set additional routing metric:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Set the additional routing metric to be added for incoming RIP routes on this interface	**rip metricin** *value*	Optional 0 by default
Set the additional routing metric to be added for outgoing RIP routes on this interface	**rip metricout** *value*	Optional 1 by default

Note

The **rip metricout** command takes effect only on the RIP routes learnt by the router and the RIP routes generated by the router itself, but the command is invalid for any route imported to RIP from other routing protocols.

Configuring RIP route summarization

Rip route summarization means that when the router advertises RIP updates, different subnet routes in the same natural network segment can be aggregated into one route with a natural mask for transmission to another network segment. This function is used to reduce the routing traffic on the network as well as the size of the routing table.

When it is necessary to advertise RIP route updates in a subnet, disable the route summarization for RIP-2.

Follow these steps to configure RIP route summarization:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Enable RIP-2 automatic route summarization	**summary**	Required Enabled by default

Disabling the router from receiving host routes

In some special cases, the router can receive a lot of host routes from the same segment, and these routes are of little help in route addressing but consume a lot of network resources. After a router is disabled from receiving host routes, it can refuse any incoming host route.

Follow these steps to disable the router from receiving host routes:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Disable the router from receiving host routes	**undo host-route**	Required By default, the router receives host routes.

Configuring RIP to filter incoming/outgoing routes

The route filtering function provided by a router enables you to configure inbound/outbound filter policy by specifying an ACL, address prefix list, or route policy to make RIP filter incoming/outgoing routes. Besides, you can configure RIP to receive only the RIP packets from a specific neighbor.

Follow these steps to configure RIP to filter incoming/outgoing routes:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Configure RIP to filter incoming routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] | **route-policy** *route-policy-name* } **import**	Required By default, RIP does not filter any incoming route. The **gateway** keyword is used to filter the incoming routes advertised from a specified address.
	filter-policy gateway *ip-prefix-name* **import**	
Configure RIP to filter outgoing routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]	Required By default, RIP does not filter any outgoing route.
	filter-policy route-policy *route-policy-name* **export**	

Note

- The **filter-policy import** command filters the RIP routes received from neighbors, and the routes being filtered out will neither be added to the routing table nor be advertised to any neighbors.
- The **filter-policy export** command filters all the routes to be advertised, including the routes redistributed with the **import-route** command and routes learned from neighbors.
- You can also use the **filter-policy export** command to filter outgoing routes redistributed from a specified routing protocol.

Setting RIP preference

Follow these steps to set RIP preference:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Set the RIP preference	**preference** *value*	Required 100 by default

Enabling load sharing among RIP interfaces

Follow these steps to enable load sharing among RIP interfaces:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Enable load sharing among RIP interfaces	**traffic-share-across-interface**	Required Disabled by default

Configuring RIP to redistribute routes from another protocol

Follow these steps to configure RIP to import routes from another protocol:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Configure a default cost for an incoming route	**default cost** *value*	Optional 1 by default
Configure RIP to redistribute routes from another protocol	**import-route** *protocol* [**cost** *value* | **route-policy** *route-policy-name*]*	Required By default, RIP does not redistribute any route from other protocols.

RIP Network Adjustment and Optimization

In some special network environments, some RIP features need to be configured and RIP network performance needs to be adjusted and optimized. By performing the configuration mentioned in this section, the following can be implemented:

- Changing the convergence speed of RIP network by adjusting RIP timers;
- Avoiding routing loops by configuring split horizon;
- Packet validation in network environments with high security requirements, and
- Configuring RIP to unicast RIP messages on interfaces with special requirements.

Configuration Prerequisites

Before adjusting RIP, perform the following tasks:

- Configuring the network layer addresses of interfaces so that adjacent nodes are reachable to each other at the network layer
- Configuring basic RIP functions

Configuration Tasks

Configuring RIP timers

Follow these steps to configure RIP timers:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Set the RIP timers	**timers** { **update** *update-timer* | **timeout** *timeout-timer* } *	Required By default, the Update timer is 30 seconds and the Timeout timer 180 seconds.

Note

When configuring the values of RIP timers, you should take network performance into consideration and perform consistent configuration on all routers running RIP to avoid unnecessary network traffic and network route oscillation.

Configuring split horizon

Follow these steps to configure split horizon:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Enable split horizon	**rip split-horizon**	Required Enabled by default

Note

Split horizon cannot be disabled on a point-to-point link.

Configuring RIP-1 packet zero field check

Follow these steps to configure RIP-1 packet zero field check:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Enable the check of the **must be zero** field in RIP-1 packets	**checkzero**	Required Enabled by default

Note

Some fields in a RIP-1 packet must be 0, and they are known as **must be zero** field. For RIP-1, the **must be zero** field is checked for incoming packets, and those RIP-1 packets with this field being nonzero will not be processed.

Setting RIP-2 packet authentication mode

RIP-2 supports two authentication modes: simple authentication and message digest 5 (MD5) authentication.

Simple authentication cannot provide complete security, because the authentication keys sent along with packets that are not encrypted. Therefore, simple authentication cannot be applied where high security is required.

Follow these steps to set RIP-2 packet authentication mode:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	—
Set RIP-2 packet authentication mode	**rip authentication-mode** { **simple** *password* | **md5** { **rfc2082** *key-string key-id* | **rfc2453** *key-string* } }	Required If you specify to use MD5 authentication, you must specify one of the following MD5 authentication types: • rfc2453 (this type supports the packet format defined in RFC 2453) • rfc2082 (this type supports the packet format defined in RFC 2082)

Configuring RIP to unicast RIP packets

Follow these steps to configure RIP to unicast RIP packets:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter RIP view	**rip**	—
Configure RIP to unicast RIP packets	**peer** *ip-address*	Required When RIP runs on the link that does not support broadcast or multicast, you must configure RIP to unicast RIP packets.

Displaying and Maintaining RIP Configuration

To do...	Use the command...	Remarks
Display the current RIP running status and configuration information	**display rip**	Available in any view
Display RIP interface information	**display rip interface**	
Display RIP routing information	**display rip routing**	
Reset the system configuration related to RIP	**reset**	Available in RIP view

RIP Configuration Example

Network requirements

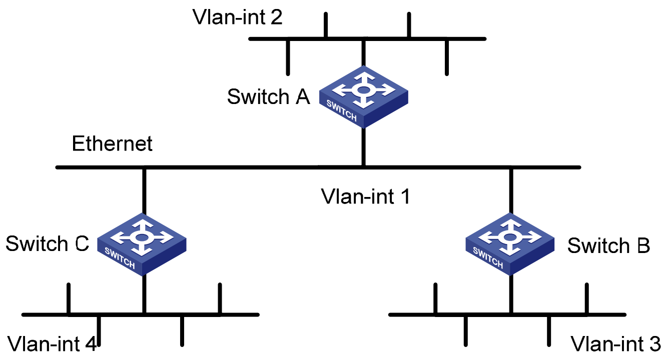
A small-sized company requires that any two nodes in its small office network communicate with each other, and that the network devices automatically adapt themselves to any topology change so as to reduce the work of manual maintenance.

In this case, RIP can implement communication between any two nodes.

Network diagram

According to the network requirements, the network topology is designed as shown in Figure 3-1.

Figure 3-1 Network diagram for RIP configuration



Device	Interface	IP address	Device	Interface	IP address
Switch A	Vlan-int1	110.11.2.1/24	Switch B	Vlan-int1	110.11.2.2/24
	Vlan-int2	155.10.1.1/24		Vlan-int3	196.38.165.1/24

Switch C	Vlan-int1	110.11.2.3/24			
	Vlan-int4	117.102.0.1/16			

Configuration procedure

Note

Only the configuration related to RIP is listed below. Before the following configuration, make sure the Ethernet link layer works normally and the IP addresses of VLAN interfaces are configured correctly.

1) Configure Switch A:

Configure RIP.

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip] network 110.11.2.0
[SwitchA-rip] network 155.10.1.0
```

2) Configure Switch B:

Configure RIP.

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip] network 196.38.165.0
[SwitchB-rip] network 110.11.2.0
```

3) Configure Switch C:

Configure RIP.

```
<SwitchC> system-view
[SwitchC] rip
[SwitchC-rip] network 117.102.0.0
[SwitchC-rip] network 110.11.2.0
```

Troubleshooting RIP Configuration

Failed to Receive RIP Updates

Symptom

The Ethernet switch cannot receive any RIP update when the physical connection between the switch and the peer routing device is normal.

Solution

Check that:

- RIP is enabled by using the **network** command on the corresponding interface.
- The interface is allowed to receive or send RIP packets.
- The interface receives RIP packets in the way the peer device sends them, for example, in the broadcast or multicast mode.

4 IP Route Policy Configuration

When configuring an IP route policy, go to these sections for information you are interested in:

Note

The term **router** in this chapter refers to a router in a generic sense or an Ethernet switch running a routing protocol.

IP Route Policy Overview

Introduction to IP Route Policy

Route policy is technology used to modify routing information to control the forwarding path of data packets. Route policy is implemented by changing the route attributes such as reachability.

When a router distributes or receives routing information, it may need to implement some policies to filter the routing information, so as to receive or distribute only the routing information meeting given conditions. A routing protocol (RIP, for example) may need to import the routing information discovered by other protocols to enrich its routing knowledge. While importing routing information from another protocol, it possibly only needs to import the routes meeting given conditions and control some attributes of the imported routes to make the routes meet the requirements of this protocol.

For the implementation of a route policy, you need to define a set of matching rules by specifying the characteristics of the routing information to be filtered. You can set the rules based on such attributes as destination address and source address of the information. The matching rules can be set in advance and then used in the routing policies to advertise, receive, and import routes.

Filters

A routing protocol can reference an ACL, IP-prefix, or route policy to filter routing information. The following sections describe these filters.

ACL

You can specify a range of IP addresses or subnets when defining an ACL so as to match the destination network addresses or next-hop addresses in routing information. You can reference an ACL into a route policy to filter routing information.

For ACL configuration, refer to the part discussing ACL.

IP-prefix list

IP-prefix list plays a role similar to ACL. But it is more flexible than ACL and easier to understand. When IP-prefix list is applied to filter routing information, its matching object is the destination address field in routing information. Moreover, with IP-prefix list, you can use the **gateway** option to specify that only routing information advertised by certain routers will be received.

An IP-prefix list is identified by its IP-prefix name. Each IP-prefix list can contain multiple entries, and each entry, identified by an index-number, can independently specify the match range in the network prefix form. An index-number specifies the matching sequence in the IP-prefix list.

There is an OR relationship between entries. During the matching, the router checks entries identified by index-number in ascending order. Once an entry is matched, the IP-prefix list filtering is passed and no other entries will be checked.

Route policy

A route policy is used to match some attributes with given routing information and the attributes of the information will be set if the conditions are satisfied.

A route policy can comprise multiple nodes. Each node is a unit for matching test, and the nodes will be matched in ascending order of their node numbers. Each node comprises a set of **if-match** and **apply** clauses. The **if-match** clauses define the matching rules. The matching objects are some attributes of routing information. The relationship among the **if-match** clauses for a node is “AND”. As a result, a matching test against a node is successful only when all the matching conditions specified by the **if-match** clauses in the node are satisfied. The **apply** clauses specify the actions performed after a matching test against the node is successful, and the actions can be the attribute settings of routing information.

There is an OR relationship between different nodes in a route policy. As a result, the system examines the nodes in the route policy in sequence, and once the route matches a node in the route policy, it will pass the matching test of the route policy without entering the test of the next node.

IP Route Policy Configuration Task List

Complete the following tasks to configure an IP route policy:

Task		Remarks
Route Policy Configuration	Defining a Route Policy	Required
	Defining if-match Clauses and apply Clauses	Required
IP-Prefix Configuration		Required

Route Policy Configuration

A route policy is used to match given routing information or some attributes of routing information and change the attributes of the routing information if the conditions are met. The above-mentioned filtering lists can serve as the match conditions:

A route policy can comprise multiple nodes and each node comprises:

- **if-match** clause: Defines matching rules; that is, the filtering conditions that the routing information should satisfy for passing the current route policy. The matching objects are some attributes of the routing information.
- **apply** clause: Specifies actions, which are the configuration commands executed after a route satisfies the filtering conditions specified by the **if-match** clause. Thereby, some attributes of the route can be modified.

Configuration Prerequisites

Before configuring a route policy, perform the following tasks:

- Configuring a filtering list,
- Configuring a routing protocol

Prepare the following data before the configuration:

- Route policy name and node number
- Match conditions
- Route attributes to be changed

Defining a Route Policy

Follow these steps to define a route policy:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Define a route policy and enter the route policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required Not defined by default

Note

- The **permit** argument specifies the matching mode for a defined node in the route policy to be in **permit** mode. If a route matches the rules for the node, the **apply** clauses for the node will be executed and the test of the next node will not be taken. If not, however, the route takes the test of the next node.
- The **deny** argument specifies the matching mode for a defined node in the route policy to be in **deny** mode. In this mode, no **apply** clause is executed. If a route satisfies all the **if-match** clauses of the node, no **apply** clause for the node will be executed and the test of the next node will not be taken. If not, however, the route takes the test of the next node.
- If multiple nodes are defined in a route policy, at least one of them should be in **permit** mode. When a route policy is applied to filtering routing information, if a piece of routing information does not match any node, the routing information will be denied by the route policy. If all the nodes in the route policy are in **deny** mode, all routing information will be denied by the route policy.

Defining if-match Clauses and apply Clauses

Follow these steps to define if-match clauses and apply clauses:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter the route-policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*	Required
Define a rule to match the IP address of routing information	**if-match** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	Optional By default, no matching is performed on the address of routing information.
Define a rule to match the cost of routes	**if-match cost** *value*	Optional By default, no matching is performed against the cost of routes.
Define a rule to match the next-hop interface of routing information	**if-match interface** *interface-type* *interface-number*	Optional By default, no matching is performed on the next-hop interface of routing information.
Define a rule to match the next-hop address of routing information	**if-match ip next-hop** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }	Optional By default, no matching is performed on the next-hop address of routing information.
Define a rule to match the tag field of routing information	**if-match tag** *value*	Optional By default, no matching is performed on the tag field of routing information.
Apply a cost to routes satisfying matching rules	**apply cost** *value*	Optional By default, no cost is applied to routes satisfying matching rules.
Define an action to set the tag field of routing information	**apply tag** *value*	Optional By default, no action is defined to set the tag field of routing information.

Note

- A route policy comprises multiple nodes. There is an OR relationship between the nodes in a route policy. As a result, the system examines the nodes in sequence, and once the route matches a node in the route policy, it will pass the matching test of the route policy without entering the test of the next node.
- During the matching, there is an AND relationship between the **if-match** clauses for a route policy node. That is, a matching test against a node is successful only when all the matching conditions specified by the **if-match** clauses in the node are satisfied.
- If no **if-match** clauses are specified, all the routes will filter through the node.
- A node can comprise no **if-match** clause or multiple **if-match** clauses.
- Each node comprises a set of **if-match** and **apply** clauses. **if-match** clauses define matching rules. **apply** clauses specify the actions performed after a matching test against the node is successful, and the actions can be the attribute settings of routing information.

IP-Prefix Configuration

IP-prefix plays a role similar to ACL and but is more flexible and easier to understand. When IP-prefix is applied to filtering routing information, its matching object is the destination address information field of routing information.

Configuration Prerequisites

Before configuring a filter list, prepare the following data:

- IP-prefix name
- Range of addresses to be matched

Configuring an ip-prefix list

An IP-prefix list is identified by its IP-prefix list name. Each IP-prefix list can comprise multiple entries. Each entry can independently specify a match range in the form of network prefix and is identified by an index-number. For example, the following is an IP-prefix list named **abcd**:

- ip ip-prefix abcd index 10 permit 1.0.0.0 8
- ip ip-prefix abcd index 20 permit 2.0.0.0 8

During the matching of a route, the router checks the entries in ascending order of index-number. Once the route matches an entry, the route passes the filtering of the IP-prefix list and no other entry will be matched.

Follow these steps to configure an IPv4 IP-prefix list:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure an IPv4 IP-prefix list	**ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *network len* [**greater-equal** *greater-equal* | **less-equal** *less-equal*]	Required Not configured by default

Note

If all the entries of the IP prefix list are in the **deny** mode, all routing information will be denied by the filter. In this case, you are recommended to define an entry in the **permit** mode with the **ip ip-prefix** *ip-prefix-name* **index** *index-number* **permit** 0.0.0.0 0 **less-equal** 32 command following multiple entries in the **deny** mode to permit all the other IP routes.

Displaying IP Route Policy

To do...	Use the command...	Remarks
Display route policy information	**display route-policy** [*route-policy-name*]	Available in any view
Display IP-prefix information	**display ip ip-prefix** [*ip-prefix-name*]	

IP Route Policy Configuration Example

Controlling RIP Packet Cost to Implement Dynamic Route Backup

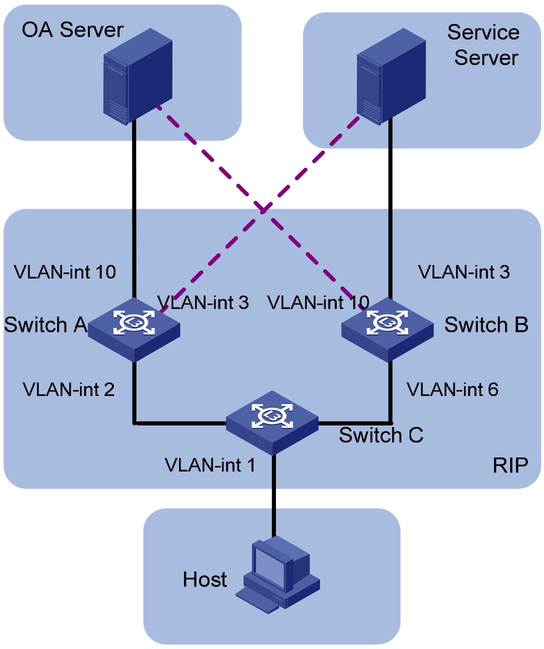
Network requirements

The required speed of convergence in the small network of a company is not high. The network provides two services. Main and backup links are provided for each service for the purpose of reliability. The main link of one service serves as the backup link of the other. The two services are distinguished by IP addresses. If a fault occurs to the main link of one service, dynamic backup can prevent service interruption.

Network diagram

According to the network requirements, the network topology is designed as shown in Figure 4-1.

Figure 4-1 Network diagram



Device	Interface	IP address
Switch A	Vlan-int 2	2.2.2.1/8
	Vlan-int 3	3.3.3.254/8
	Vlan-int 10	1.1.1.254/8
Switch B	Vlan-int 3	3.3.3.253/8
	Vlan-int 6	6.6.6.5/8
	Vlan-int 10	1.1.1.253/8
Switch C	Vlan-int 1	192.168.0.39/24
	Vlan-int 2	2.2.2.2/8
	Vlan-int 6	6.6.6.6/8
OA Server		1.1.1.1/32
Service Server		3.3.3.3/32
Host		192.168.0.9/24

Configuration considerations

- According to the network requirements, select RIP.

- For the OA server, the main link is between Switch A and Switch C, while the backup link is between Switch B and Switch C.
- For the service server, the main link is between Switch B and Switch C, while the backup link is between Switch A and Switch C.
- Apply a route policy to control the cost of routes received by Switch C to provide main and backup links for the services of the OA server and service server.

Configuration procedure

1) Configure Switch A.

Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

Configure RIP.

```
<SwitchA> system-view
[SwitchA] rip
[SwitchA-rip] network 1.0.0.0
[SwitchA-rip] network 2.0.0.0
[SwitchA-rip] network 3.0.0.0
```

2) Configure Switch B.

Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

Configure RIP.

```
<SwitchB> system-view
[SwitchB] rip
[SwitchB-rip] network 1.0.0.0
[SwitchB-rip] network 3.0.0.0
[SwitchB-rip] network 6.0.0.0
```

3) Configure Switch C.

Create VLANs and configure IP addresses for the VLAN interfaces. The configuration procedure is omitted.

Define IP-prefix 1 containing the IP address prefix 1.0.0.0/8, and IP-prefix 2 containing the IP address prefix 3.0.0.0/8.

```
<SwitchC> system-view
[SwitchC] ip ip-prefix 1 index 10 permit 1.0.0.0 8
[SwitchC] ip ip-prefix 2 index 10 permit 3.0.0.0 8
```

Create a route policy named **in** and node 10 with the matching mode being **permit**. Define if-match clauses. Apply the cost 5 to routes matching the outgoing interface VLAN-interface 2 and prefix list 1.

```
[SwitchC] route-policy in permit node 10
[SwitchC-route-policy] if-match interface Vlan-interface2
[SwitchC-route-policy] if-match ip-prefix 1
[SwitchC-route-policy] apply cost 5
[SwitchC-route-policy] quit
```

Create node 20 with the matching mode being **permit** in the route policy. Define if-match clauses. Apply the cost 6 to routes matching the outgoing interface VLAN-interface 2 and prefix list 2.

```
[SwitchC] route-policy in permit node 20
```

```
[SwitchC-route-policy] if-match interface Vlan-interface2
[SwitchC-route-policy] if-match ip-prefix 2
[SwitchC-route-policy] apply cost 6
[SwitchC-route-policy] quit
```

Create node 30 with the matching mode being **permit** in the route policy. Define if-match clauses. Apply the cost 6 to routes matching the outgoing interface VLAN-interface 6 and prefix list 1.

```
[SwitchC] route-policy in permit node 30
[SwitchC-route-policy] if-match interface Vlan-interface6
[SwitchC-route-policy] if-match ip-prefix 1
[SwitchC-route-policy] apply cost 6
[SwitchC-route-policy] quit
```

Create node 40 with the matching mode being **permit** in the route policy. Define if-match clauses. Apply the cost 5 to routes matching the outgoing interface VLAN-interface 6 and prefix list 2.

```
[SwitchC] route-policy in permit node 40
[SwitchC-route-policy] if-match interface Vlan-interface6
[SwitchC-route-policy] if-match ip-prefix 2
[SwitchC-route-policy] apply cost 5
[SwitchC-route-policy] quit
```

Create node 50 with the matching mode being **permit**, to allow all routing information to pass.

```
[SwitchC] route-policy in permit node 50
[SwitchC-route-policy] quit
```

Configure RIP and apply the route policy **in** to the incoming routing information.

```
[SwitchC] rip
[SwitchC-rip] network 1.0.0.0
[SwitchC-rip] network 3.0.0.0
[SwitchC-rip] network 6.0.0.0
[SwitchC-rip] filter-policy route-policy in import
```

Configuration verification

1) Display data forwarding paths when the main link of the OA server between Switch A and Switch C works normally.

```
<SwitchC> display ip routing-table
 Routing Table: public net
Destination/Mask    Protocol   Pre  Cost    Nexthop      Interface
1.0.0.0/8             RIP        100  5       2.2.2.1        Vlan-interface2
2.0.0.0/8         DIRECT     0    0       2.2.2.2        Vlan-interface2
2.2.2.2/32        DIRECT     0    0       127.0.0.1      InLoopBack0
3.0.0.0/8             RIP        100  5       6.6.6.5        Vlan-interface6
6.0.0.0/8         DIRECT     0    0       6.6.6.6        Vlan-interface6
6.6.6.6/32            DIRECT     0    0       127.0.0.1      InLoopBack0
127.0.0.0/8           DIRECT     0    0       127.0.0.1      InLoopBack0
127.0.0.1/32          DIRECT     0    0       127.0.0.1      InLoopBack0
192.168.0.0/24       DIRECT     0    0       192.168.0.39   Vlan-interface1
192.168.0.39/32     DIRECT     0    0       127.0.0.1      InLoopBack0
```

2) Display data forwarding paths when the main link of the OA server between Switch A and Switch C is down.

```
<SwitchC> display ip routing-table
 Routing Table: public net
Destination/Mask     Protocol    Pre  Cost     Nexthop       Interface
1.0.0.0/8             RIP         100   6        6.6.6.5        Vlan-interface2
3.0.0.0/8             RIP         100   5        6.6.6.5        Vlan-interface6
6.0.0.0/8         DIRECT      0     0        6.6.6.6        Vlan-interface6
6.6.6.6/32            DIRECT      0     0        127.0.0.1      InLoopBack0
127.0.0.0/8           DIRECT      0     0        127.0.0.1      InLoopBack0
127.0.0.1/32          DIRECT      0     0        127.0.0.1      InLoopBack0
192.168.0.0/24        DIRECT      0     0        192.168.0.39   Vlan-interface1
192.168.0.39/32      DIRECT      0     0        127.0.0.1       InLoopBack0
```

Precautions

1) When you configure the **apply cost** command in a route policy:

- The new cost should be greater than the original one to prevent RIP from generating routing loop in the case that a loop exists in the topology.
- The cost will become 16 if you try to set it to a value greater than 16.
- The cost will become the original one if you try to set it to 0.
- The cost will still be 16 if you try to set it to 16.

2) Using the **if-match interface** command will match the routes whose outgoing interface to the next hop is the specified interface.

3) You are recommended to configure a node to match all routes not passing the preceding nodes in a route policy.

4) If the cost of a received RIP route is equal to 16, the cost specified by the **apply cost** command in a route policy will not be applied to the route, that is, the cost of the route is equal to 16.

5) Using the **filter-policy** command does not filter redistributed routes.

Troubleshooting IP Route Policy

Symptom

The route policy cannot filter routing information correctly when the routing protocol runs normally.

Analysis

The route policy cannot filter routing information correctly in the following two cases:

- All nodes in the route policy are in the **deny** mode.
- All entries in the IP-prefix list are in the **deny** mode.

Solution

1) Use the **display ip ip-prefix** command to display the configuration of the IP-prefix list.

2) Use the **display route-policy** command to display the configuration of the route policy.

Table of Contents

1 Multicast Overview

Note

In this manual, the term “router” refers to a router in the generic sense or a Layer 3 Ethernet switch running an IP multicast protocol.

Multicast Overview

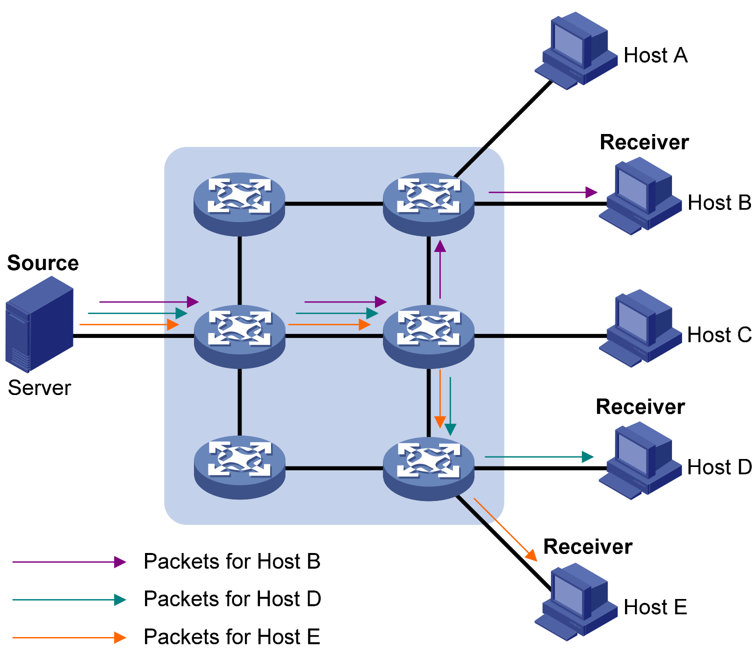
With the development of the Internet, more and more interaction services such as data, voice, and video services are running on the network. In addition, highly bandwidth- and time-critical services, such as e-commerce, Web conferencing, online auctions, video on demand (VoD), and tele-education have come into being. These services have higher requirements for information security, legal use of paid services, and network bandwidth.

In the network, packets are sent in three modes: unicast, broadcast and multicast. The following sections describe and compare data interaction processes for unicast, broadcast, and multicast traffic.

Information Transmission in the Unicast Mode

In unicast, the system establishes a separate data transmission channel for each user requiring this information, and sends a separate copy of the information to the user, as shown in Figure 1-1:

Figure 1-1 Information transmission in the unicast mode

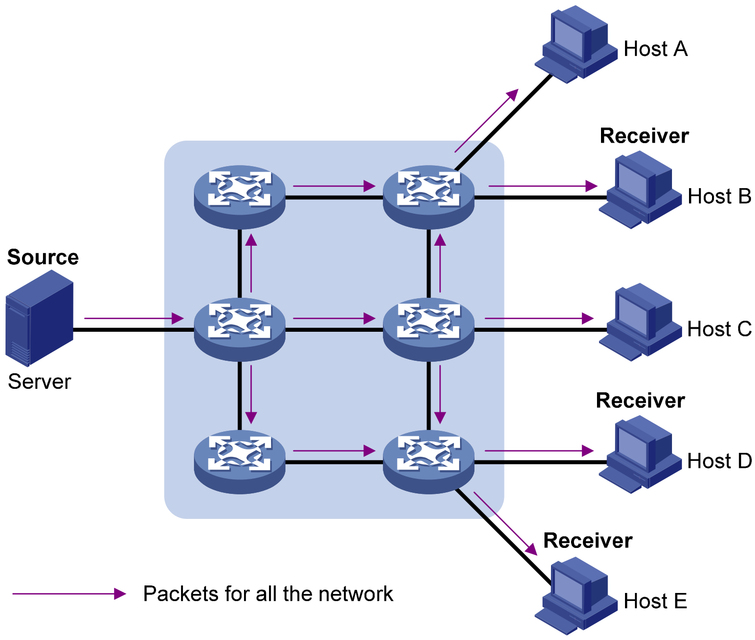


Assume that Hosts B, D and E need this information. The source server establishes transmission channels for the devices of these users respectively. As the transmitted traffic over the network is in direct proportion to the number of users that receive this information, when a large number of users need the same information, the server must send many packets of information with the same content to the users. While suitable for networks with small numbers of users, or where information transmitted to users is significantly different, in other cases this is an inefficient use of the network, and when there is limited bandwidth, bottlenecks can develop in information transmission. In general, unicast is not good for the transmission of a great deal of the same information to multiple recipients.

Information Transmission in the Broadcast Mode

When you broadcast traffic, the system transmits information to all users on a network. Any user on the network can receive the information, no matter if the information is needed or not. Figure 1-2 shows information transmission in broadcast mode.

Figure 1-2 Information transmission in the broadcast mode



Assume that Hosts B, D, and E need the information. The source server broadcasts this information through the routers, reaching the targets, but also Hosts A and C on the network receive this information.

This is an efficient way to send the same content to densely distributed users. However, as we can see from the information transmission process, security and restricted use of paid services cannot be guaranteed. In addition, when only a small number of users on the same network need the information, the utilization ratio of the network resources is very low and the bandwidth resources are greatly wasted.

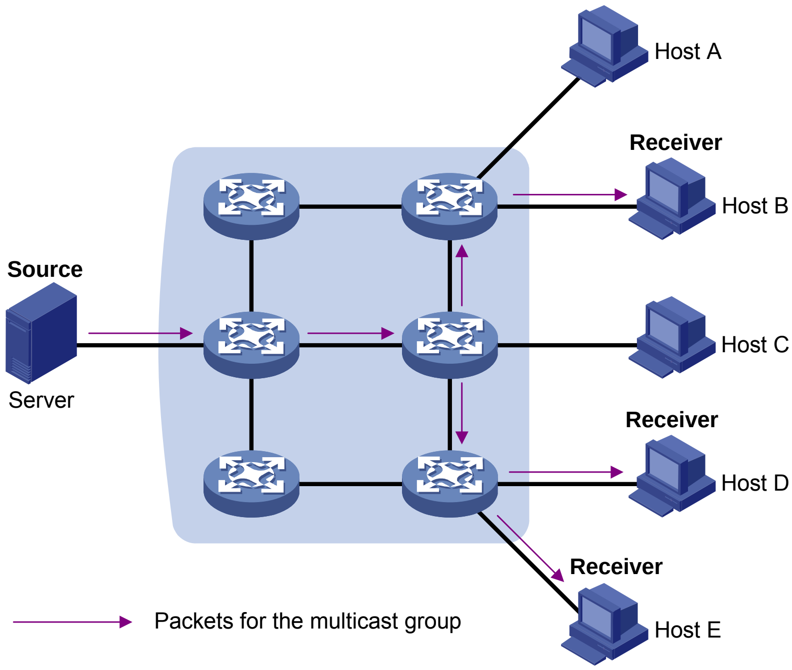
Therefore, broadcast is disadvantageous in transmitting data to specific users, and is more bandwidth intensive.

Information Transmission in the Multicast Mode

As described in the previous sections, unicast is suitable for networks with sparsely distributed users, whereas broadcast is suitable for networks with densely distributed users. When the number of users requiring information is not certain, unicast and broadcast not efficient.

Multicast solves this problem. When some users on a network require specified information, the multicast information sender (namely, the multicast source) sends the information only once. With multicast distribution trees established for multicast data packets through multicast routing protocols, the packets are duplicated and distributed at the nearest nodes, as shown in Figure 1-3:

Figure 1-3 Information transmission in the multicast mode



Assume that Hosts B, D and E need the information. To transmit the information to the right users, it is necessary to group Hosts B, D and E into a receiver set. The routers on the network duplicate and distribute the information based on the distribution of the receivers in this set. Finally, the information is correctly delivered to Hosts B, D, and E.

The advantages of multicast over unicast are as follows:

- No matter how many receivers exist, there is only one copy of the same multicast data flow on each link.
- With the multicast mode used to transmit information, an increase of the number of users does not add to the network burden remarkably.

The advantages of multicast over broadcast are as follows:

- A multicast data flow can be sent only to the receiver that requires the data.
- Multicast brings no waste of network resources and makes proper use of bandwidth.

Roles in Multicast

The following roles are involved in multicast transmission:

- An information sender is referred to as a multicast source (“Source” in Figure 1-3).
- Each receiver is a multicast group member (“Receiver” in Figure 1-3).

- All receivers interested in the same information form a multicast group. Multicast groups are not subject to geographic restrictions.
- A router that supports Layer 3 multicast is called multicast router or Layer 3 multicast device. In addition to providing multicast routing, a multicast router can also manage multicast group members.

For a better understanding of the multicast concept, you can use the analogy of a transmission of TV programs, as shown in Table 1-1.

Table 1-1 An analogy between TV transmission and multicast transmission

Step	TV transmission	Multicast transmission
1	A TV station transmits a TV program through a television channel.	A multicast source sends multicast data to a multicast group.
2	A user tunes the TV set to the channel.	A receiver joins the multicast group.
3	The user starts to watch the TV program transmitted by the TV station via the channel.	The receiver starts to receive the multicast data that the source sends to the multicast group.
4	The user turns off the TV set.	The receiver leaves the multicast group.

Note

- A multicast source does not necessarily belong to a multicast group. Namely, a multicast source is not necessarily a multicast data receiver.
- A multicast source can send data to multiple multicast groups at the same time, and multiple multicast sources can send data to the same multicast group at the same time.

Common Notations in Multicast

Two notations are commonly used in multicast:

- (*, G): Indicates a rendezvous point tree (RPT), or a multicast packet that any multicast source sends to multicast group G. Here "*" represents any multicast source, while "G" represents a specific multicast group.
- (S, G): Indicates a shortest path tree (SPT), or a multicast packet that multicast source S sends to multicast group G. Here "S" represents a specific multicast source, while "G" represents a specific multicast group.

Advantages and Applications of Multicast

Advantages of multicast

Advantages of multicast include:

- Enhanced efficiency: Multicast decreases network traffic and reduces server load and CPU load.
- Optimal performance: Multicast reduces redundant traffic.

- Distributive application: Multicast makes multiple-point application possible.

Application of multicast

The multicast technology effectively addresses the issue of point-to-multipoint data transmission. By enabling high-efficiency point-to-multipoint data transmission, over an IP network, multicast greatly saves network bandwidth and reduces network load.

Multicast provides the following applications:

- Applications of multimedia and flow media, such as Web TV, Web radio, and real-time video/audio conferencing.
- Communication for training and cooperative operations, such as remote education.
- Database and financial applications (stock), and so on.
- Any point-to-multiple-point data application.

Multicast Models

Based on the multicast source processing modes, there are three multicast models:

- Any-source multicast (ASM)
- Source-filtered multicast (SFM)
- Source-specific multicast (SSM)

ASM model

In the ASM model, any sender can become a multicast source and send information to a multicast group; numbers of receivers can join a multicast group identified by a group address and obtain multicast information addressed to that multicast group. In this model, receivers are not aware of the position of a multicast source in advance. However, they can join or leave the multicast group at any time.

SFM model

The SFM model is derived from the ASM model. From the view of a sender, the two models have the same multicast group membership architecture.

Functionally, the SFM model is an extension of the ASM model. In the SFM model, the upper layer software checks the source address of received multicast packets so as to permit or deny multicast traffic from specific sources. Therefore, receivers can receive the multicast data from only part of the multicast sources. From the view of a receiver, multicast sources are not all valid: they are filtered.

SSM model

In the practical life, users may be interested in the multicast data from only certain multicast sources. The SSM model provides a transmission service that allows users to specify the multicast sources they are interested in at the client side.

The radical difference between the SSM model and the ASM model is that in the SSM model, receivers already know the locations of the multicast sources by some means. In addition, the SSM model uses a multicast address range that is different from that of the ASM model, and dedicated multicast forwarding paths are established between receivers and the specified multicast sources.

Multicast Architecture

The purpose of IP multicast is to transmit information from a multicast source to receivers in the multicast mode and to satisfy information requirements of receivers. You should be concerned about:

- Host registration: What receivers reside on the network?
- Technologies of discovering a multicast source: Which multicast source should the receivers receive information from?
- Multicast addressing mechanism: Where should the multicast source transports information?
- Multicast routing: How is information transported?

IP multicast is a kind of peer-to-peer service. Based on the protocol layer sequence from bottom to top, the multicast mechanism contains addressing mechanism, host registration, multicast routing, and multicast application:

- Addressing mechanism: Information is sent from a multicast source to a group of receivers through multicast addresses.
- Host registration: A receiving host joins and leaves a multicast group dynamically using the membership registration mechanism.
- Multicast routing: A router or switch transports packets from a multicast source to receivers by building a multicast distribution tree with multicast routes.
- Multicast application: A multicast source must support multicast applications, such as video conferencing. The TCP/IP protocol suite must support the function of sending and receiving multicast information.

Multicast Address

As receivers are multiple hosts in a multicast group, you should be concerned about the following questions:

- What destination should the information source send the information to in the multicast mode?
- How to select the destination address?

These questions are about multicast addressing. To enable the communication between the information source and members of a multicast group (a group of information receivers), network-layer multicast addresses, namely, IP multicast addresses must be provided. In addition, a technology must be available to map IP multicast addresses to link-layer MAC multicast addresses. The following sections describe these two types of multicast addresses:

IP multicast address

Internet Assigned Numbers Authority (IANA) categorizes IP addresses into five classes: A, B, C, D, and E. Unicast packets use IP addresses of Class A, B, and C based on network scales. Class D IP addresses are used as destination addresses of multicast packets. Class D address must not appear in the IP address field of a source IP address of IP packets. Class E IP addresses are reserved for future use.

In unicast data transport, a data packet is transported hop by hop from the source address to the destination address. In an IP multicast environment, there are a group of destination addresses (called group address), rather than one address. All the receivers join a group. Once they join the group, the data sent to this group of addresses starts to be transported to the receivers. All the members in this group can receive the data packets. This group is a multicast group.

A multicast group has the following characteristics:

- The membership of a group is dynamic. A host can join and leave a multicast group at any time.
- A multicast group can be either permanent or temporary.
- A multicast group whose addresses are assigned by IANA is a permanent multicast group. It is also called reserved multicast group.

Note that:

- The IP addresses of a permanent multicast group keep unchanged, while the members of the group can be changed.
- There can be any number of, or even zero, members in a permanent multicast group.
- Those IP multicast addresses not assigned to permanent multicast groups can be used by temporary multicast groups.

Class D IP addresses range from 224.0.0.0 to 239.255.255.255. For details, see Table 1-2.

Table 1-2 Range and description of Class D IP addresses

Class D address range	Description
224.0.0.0 to 224.0.0.255	Reserved multicast addresses (IP addresses for permanent multicast groups). The IP address 224.0.0.0 is reserved. Other IP addresses can be used by routing protocols.
224.0.1.0 to 231.255.255.255 233.0.0.0 to 238.255.255.255	Available any-source multicast (ASM) multicast addresses (IP addresses for temporary groups). They are valid for the entire network.
232.0.0.0 to 232.255.255.255	Available source-specific multicast (SSM) multicast group addresses.
239.0.0.0 to 239.255.255.255	Administratively scoped multicast addresses, which are for specific local use only.

As specified by IANA, the IP addresses ranging from 224.0.0.0 to 224.0.0.255 are reserved for network protocols on local networks. The following table lists commonly used reserved IP multicast addresses:

Table 1-3 Reserved IP multicast addresses

Class D address range	Description
224.0.0.1	Address of all hosts
224.0.0.2	Address of all multicast routers
224.0.0.3	Unassigned
224.0.0.4	Distance Vector Multicast Routing Protocol (DVMRP) routers
224.0.0.5	Open Shortest Path First (OSPF) routers
224.0.0.6	Open Shortest Path First designated routers (OSPF DR)
224.0.0.7	Shared tree routers
224.0.0.8	Shared tree hosts
224.0.0.9	RIP-2 routers
224.0.0.11	Mobile agents
224.0.0.12	DHCP server/relay agent

Class D address range	Description
224.0.0.13	All Protocol Independent Multicast (PIM) routers
224.0.0.14	Resource Reservation Protocol (RSVP) encapsulation
224.0.0.15	All core-based tree (CBT) routers
224.0.0.16	The specified subnetwork bandwidth management (SBM)
224.0.0.17	All SBMS
224.0.0.18	Virtual Router Redundancy Protocol (VRRP)
224.0.0.19 to 224.0.0.255	Other protocols

Note

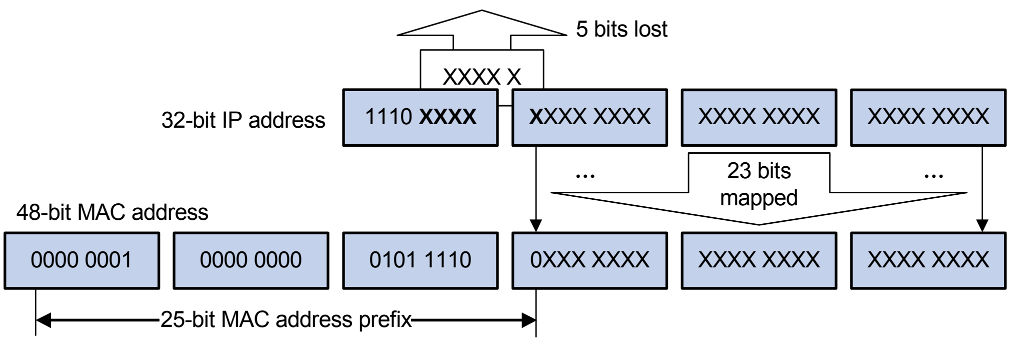
Like having reserved the private network segment 10.0.0.0/8 for unicast, IANA has also reserved the network segment 239.0.0.0/8 for multicast. These are administratively scoped addresses. With the administratively scoped addresses, you can define the range of multicast domains flexibly to isolate IP addresses between different multicast domains, so that the same multicast address can be used in different multicast domains without causing collisions.

Ethernet multicast MAC address

When a unicast IP packet is transported in an Ethernet network, the destination MAC address is the MAC address of the receiver. When a multicast packet is transported in an Ethernet network, a multicast MAC address is used as the destination address because the destination is a group with an uncertain number of members.

As stipulated by IANA, the high-order 24 bits of a multicast MAC address are 0x01005e, while the low-order 23 bits of a MAC address are the low-order 23 bits of the multicast IP address. Figure 1-4 describes the mapping relationship:

Figure 1-4 Multicast address mapping



The high-order four bits of the IP multicast address are 1110, representing the multicast ID. Only 23 bits of the remaining 28 bits are mapped to a MAC address. Thus, five bits of the multicast IP address are lost. As a result, 32 IP multicast addresses are mapped to the same MAC address.

Multicast Protocols

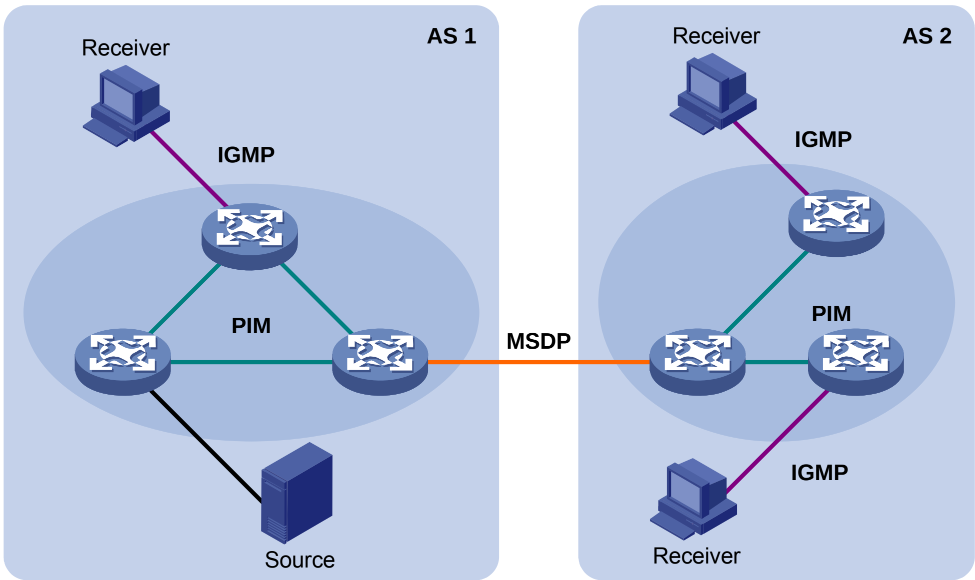
Note

- Generally, we refer to IP multicast working at the network layer as Layer 3 multicast and the corresponding multicast protocols as Layer 3 multicast protocols, which include IGMP, PIM, and MSDP; we refer to IP multicast working at the data link layer as Layer 2 multicast and the corresponding multicast protocols as Layer 2 multicast protocols, which include IGMP Snooping.
- This section provides only general descriptions about applications and functions of the Layer 2 and Layer 3 multicast protocols in a network. For details about these protocols, refer to the related chapters of this manual.

Layer 3 multicast protocols

Layer 3 multicast protocols include multicast group management protocols and multicast routing protocols. Figure 1-5 describes where these multicast protocols are in a network.

Figure 1-5 Positions of Layer 3 multicast protocols



1) Multicast management protocols

Typically, the Internet Group Management Protocol (IGMP) is used between hosts and Layer 3 multicast devices directly connected with the hosts. These protocols define the mechanism of establishing and maintaining group memberships between hosts and Layer 3 multicast devices.

2) Multicast routing protocols

A multicast routing protocol runs on Layer 3 multicast devices to establish and maintain multicast routes and forward multicast packets correctly and efficiently. Multicast routes constitute a loop-free data transmission path from a data source to multiple receivers, namely a multicast distribution tree.

In the ASM model, multicast routes come in intra-domain routes and inter-domain routes.

- An intra-domain multicast routing protocol is used to discover multicast sources and build multicast distribution trees within an autonomous system (AS) so as to deliver multicast data to receivers.

Among a variety of mature intra-domain multicast routing protocols, Protocol Independent Multicast (PIM) is a popular one. Based on the forwarding mechanism, PIM comes in two modes – dense mode (often referred to as PIM-DM) and sparse mode (often referred to as PIM-SM).

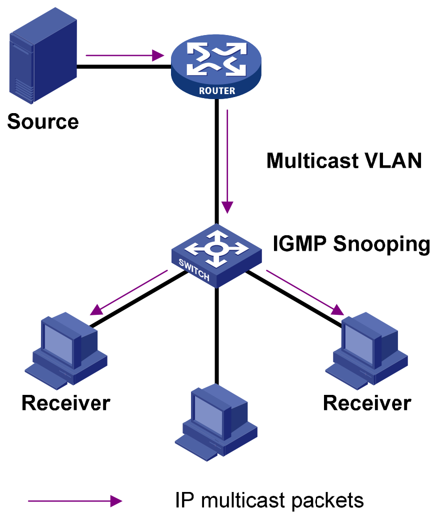
- An inter-domain multicast routing protocol is used for delivery of multicast information between two ASs. So far, mature solutions include Multicast Source Discovery Protocol (MSDP).

For the SSM model, multicast routes are not divided into inter-domain routes and intra-domain routes. Since receivers know the position of the multicast source, channels established through PIM-SM are sufficient for multicast information transport.

Layer 2 multicast protocols

Layer 2 multicast protocols include IGMP Snooping and multicast VLAN. Figure 1-6 shows where these protocols are in the network.

Figure 1-6 Positions of Layer 2 multicast protocols



1) IGMP Snooping

Running on Layer 2 devices, Internet Group Management Protocol Snooping (IGMP Snooping) are multicast constraining mechanisms that manage and control multicast groups by listening to and analyzing IGMP messages exchanged between the hosts and Layer 3 multicast devices, thus effectively controlling and limiting the flooding of multicast data in a Layer 2 network.

2) Multicast VLAN

In the traditional multicast-on-demand mode, when users in different VLANs on a Layer 2 device need multicast information, the upstream Layer 3 device needs to forward a separate copy of the multicast data to each VLAN of the Layer 2 device. With the multicast VLAN feature enabled on the Layer 2 device, the Layer 3 multicast device needs to send only one copy of multicast to the multicast VLAN on the Layer 2 device. This avoids waste of network bandwidth and extra burden on the Layer 3 device.

Multicast Packet Forwarding Mechanism

In a multicast model, a multicast source sends information to the host group identified by the multicast group address in the destination address field of the IP packets. Therefore, to deliver multicast packets to receivers located in different parts of the network, multicast routers on the forwarding path usually need to forward multicast packets received on one incoming interface to multiple outgoing interfaces. Compared with a unicast model, a multicast model is more complex in the following aspects.

- In the network, multicast packet transmission is based on the guidance of the multicast forwarding table derived from the unicast routing table or the multicast routing table specially provided for multicast.
- To process the same multicast information from different peers received on different interfaces of the same device, every multicast packet is subject to a Reverse Path Forwarding (RPF) check on the incoming interface. The result of the RPF check determines whether the packet will be forwarded or discarded. The RPF check mechanism is the basis for most multicast routing protocols to implement multicast forwarding.

The RPF mechanism enables multicast devices to forward multicast packets correctly based on the multicast route configuration. In addition, the RPF mechanism also helps avoid data loops caused by various reasons.

Implementation of the RPF Mechanism

Upon receiving a multicast packet that a multicast source S sends to a multicast group G, the multicast device first searches its multicast forwarding table:

1) If the corresponding (S, G) entry exists, and the interface on which the packet actually arrived is the incoming interface in the multicast forwarding table, the router forwards the packet to all the outgoing interfaces.
2) If the corresponding (S, G) entry exists, but the interface on which the packet actually arrived is not the incoming interface in the multicast forwarding table, the multicast packet is subject to an RPF check.

- If the result of the RPF check shows that the RPF interface is the incoming interface of the existing (S, G) entry, this means that the (S, G) entry is correct but the packet arrived from a wrong path and is to be discarded.
- If the result of the RPF check shows that the RPF interface is not the incoming interface of the existing (S, G) entry, this means that the (S, G) entry is no longer valid. The router replaces the incoming interface of the (S, G) entry with the interface on which the packet actually arrived and forwards the packet to all the outgoing interfaces.

3) If no corresponding (S, G) entry exists in the multicast forwarding table, the packet is also subject to an RPF check. The router creates an (S, G) entry based on the relevant routing information and using the RPF interface as the incoming interface, and installs the entry into the multicast forwarding table.

- If the interface on which the packet actually arrived is the RPF interface, the RPF check is successful and the router forwards the packet to all the outgoing interfaces.
- If the interface on which the packet actually arrived is not the RPF interface, the RPF check fails and the router discards the packet.

RPF Check

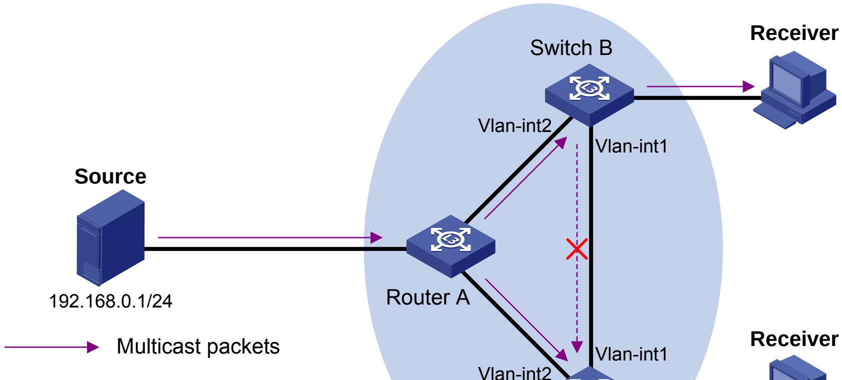
The basis for an RPF check is a unicast route. A unicast routing table contains the shortest path to each destination subnet. A multicast routing protocol does not independently maintain any type of unicast route; instead, it relies on the existing unicast routing information in creating multicast routing entries.

When performing an RPF check, a router searches its unicast routing table. The specific process is as follows: The router automatically chooses an optimal unicast route by searching its unicast routing table, using the IP address of the “packet source” as the destination address. The outgoing interface in the corresponding routing entry is the RPF interface and the next hop is the RPF neighbor. The router

considers the path along which the packet from the RPF neighbor arrived on the RPF interface to be the shortest path that leads back to the source.

Assume that unicast routes exist in the network, as shown in Figure 1-7. Multicast packets travel along the SPT from the multicast source to the receivers.

Figure 1-7 RPF check process



IP Routing Table on Switch C	
Destination/Mask	Interface
192.168.0.0/24	Vlan-int2

- A multicast packet from Source arrives to VLAN-interface 1 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. Switch C performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is VLAN-interface 2. This means that the interface on which the packet actually arrived is not the RPF interface. The RPF check fails and the packet is discarded.
- A multicast packet from Source arrives to VLAN-interface 2 of Switch C, and the corresponding forwarding entry does not exist in the multicast forwarding table of Switch C. The router performs an RPF check, and finds in its unicast routing table that the outgoing interface to 192.168.0.0/24 is the interface on which the packet actually arrived. The RPF check succeeds and the packet is forwarded.

2 Common Multicast Configuration

Note

In this manual, the term "router" refers to a router in the generic sense or a Layer 3 Ethernet switch running an IP multicast protocol.

Common Multicast Configuration

Table 2-1 Complete the following tasks to perform common multicast configurations:

Task	Remarks
Configuring Suppression on the Multicast Source Port	Optional
Configuring a Multicast MAC Address Entry	Optional
Configuring Dropping Unknown Multicast Packets	Optional

Configuring Suppression on the Multicast Source Port

Some users may deploy unauthorized multicast servers on the network. This affects the use of network bandwidth and transmission of multicast data of authorized users by taking network resources. You can configure multicast source port suppression on certain ports to prevent unauthorized multicast servers attached to these ports from sending multicast traffic to the network.

Configuring multicast source port suppression in system view

Follow these steps to configure multicast source port suppression in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure multicast source port suppression	**multicast-source-deny** [**interface** *interface-list*]	Optional Multicast source port suppression is disabled by default.

Configuring multicast source port suppression in Ethernet port view

Follow these steps to configure multicast source port suppression in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure multicast source port suppression	**multicast-source-deny**	Optional Multicast source port suppression is disabled by default.

Configuring a Multicast MAC Address Entry

In Layer 2 multicast, the system can add multicast forwarding entries dynamically through a Layer 2 multicast protocol. Alternatively, you can statically bind a port to a multicast MAC address entry by configuring a multicast MAC address entry manually.

Generally, when receiving a multicast packet for a multicast group not yet registered on the switch, the switch will flood the packet within the VLAN to which the port belongs. You can configure a static multicast MAC address entry to avoid this.

Follow these steps to configure a multicast MAC address entry in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create a multicast MAC address entry	**mac-address multicast** *mac-address* **interface** *interface-list* **vlan** *vlan-id*	Required The *mac-address* argument must be a multicast MAC address.

Follow these steps to configure a multicast MAC address entry in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Create a multicast MAC address entry.	**mac-address multicast** *mac-address* **vlan** *vlan-id*	Required The *mac-address* argument must be a multicast MAC address.

Caution

- If the multicast MAC address entry to be created already exists, the system gives you a prompt.
- If you want to add a port to a multicast MAC address entry created through the **mac-address multicast** command, you need to remove the entry first, create this entry again, and then add the specified port to the forwarding ports of this entry.
- You cannot enable link aggregation on a port on which you have configured a multicast MAC address, and you cannot configure a multicast MAC address on an aggregation port.
- You cannot configure a multicast MAC address starting with 01005e in an IGMP-Snooping-enabled VLAN. You can do that if IGMP Snooping is not enabled in the VLAN.

Configuring Dropping Unknown Multicast Packets

Generally, if the multicast address of the multicast packet received on the switch is not registered on the local switch, the packet will be flooded in the VLAN which the multicast packet belongs to. When the function of dropping unknown multicast packets is enabled, the switch will drop any multicast packets whose multicast address is not registered. Thus, the bandwidth is saved and the processing efficiency of the system is improved.

Follow these steps to configure dropping unknown multicast packet:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure dropping unknown multicast packets	**unknown-multicast drop enable**	Required By default, the function of dropping unknown multicast packets is disabled.

Displaying and Maintaining Common Multicast Configuration

Follow these commands to display common multicast configuration:

To do...	Use the command...	Remarks
Display the statistics information about multicast source port suppression	**display multicast-source-deny** [**interface** *interface-type* [*interface-number*]]	Available in any view
Display the created multicast MAC table entries	**display mac-address multicast** [**static** [[*mac-address*] **vlan** *vlan-id*] [**count**]]	Available in any view

3 IGMP Snooping Configuration

When configuring IGMP snooping, go to these sections for information you are interested in:

- IGMP Snooping Overview
- Configuring IGMP Snooping
- Displaying and Maintaining IGMP Snooping
- IGMP Snooping Configuration Examples
- Troubleshooting IGMP Snooping

Note

In this manual, the term "router" refers to a router in the generic sense or a Layer 3 Ethernet switch running an IP multicast protocol.

IGMP Snooping Overview

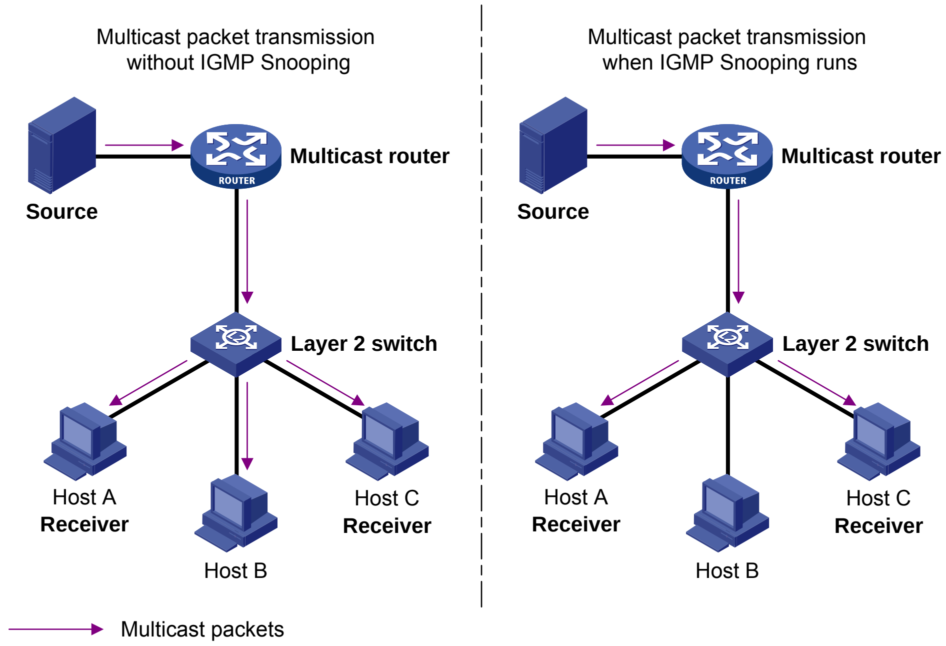
Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

Principle of IGMP Snooping

By analyzing received IGMP messages, a Layer 2 device running IGMP Snooping establishes mappings between ports and multicast MAC addresses and forwards multicast data based on these mappings.

As shown in Figure 3-1, when IGMP Snooping is not running on the switch, multicast packets are broadcast to all devices at Layer 2. When IGMP Snooping is running on the switch, multicast packets for known multicast groups are multicast to the receivers, rather than broadcast to all hosts, at Layer 2. However, multicast packets for unknown multicast groups are still broadcast at Layer 2.

Figure 3-1 Before and after IGMP Snooping is enabled on Layer 2 device

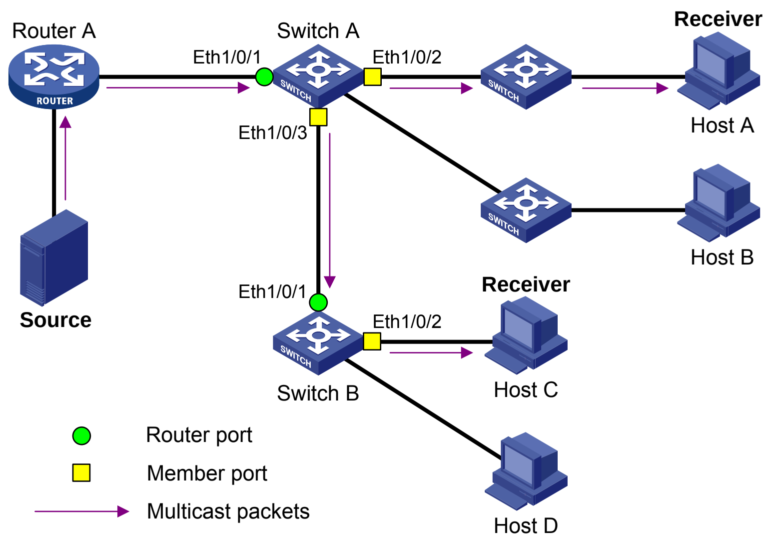


Basic Concepts in IGMP Snooping

IGMP Snooping related ports

As shown in Figure 3-2, Router A connects to the multicast source, IGMP Snooping runs on Switch A and Switch B, Host A and Host C are receiver hosts (namely, multicast group members).

Figure 3-2 IGMP Snooping related ports



Ports involved in IGMP Snooping, as shown in Figure 3-2, are described as follows:

- Router port: A router port is a port on the Layer 3 multicast device (DR or IGMP querier) side of the Ethernet switch. In the figure, Ethernet 1/0/1 of Switch A and Ethernet 1/0/1 of Switch B are router ports. A switch registers all its local router ports in its router port list.
- Member port: A member port is a port on the multicast group member side of the Ethernet switch. In the figure, Ethernet 1/0/2 and Ethernet 1/0/3 of Switch A and Ethernet 1/0/2 of Switch B are

member ports. The switch records all member ports on the local device in the IGMP Snooping forwarding table.

Port aging timers in IGMP Snooping and related messages and actions

Table 3-1 Port aging timers in IGMP Snooping and related messages and actions

Timer	Description	Message before expiry	Action after expiry
Router port aging timer	For each router port, the switch sets a timer initialized to the aging time of the route port	IGMP general query or PIM hello	The switch removes this port from its router port list
Member port aging timer	When a port joins a multicast group, the switch sets a timer for the port, which is initialized to the member port aging time	IGMP membership report	The switch removes this port from the multicast group forwarding table

Work Mechanism of IGMP Snooping

A switch running IGMP Snooping performs different actions when it receives different IGMP messages, as follows:

When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local subnet to find out whether active multicast group members exist on the subnet.

Upon receiving an IGMP general query, the switch forwards it through all ports in the VLAN except the receiving port and performs the following to the receiving port:

- If the receiving port is a router port existing in its router port list, the switch resets the aging timer of this router port.
- If the receiving port is not a router port existing in its router port list, the switch adds it into its router port list and sets an aging timer for this router port.

When receiving a membership report

A host sends an IGMP report to the multicast router in the following circumstances:

- Upon receiving an IGMP query, a multicast group member host responds with an IGMP report.
- When intended to join a multicast group, a host sends an IGMP report to the multicast router to announce that it is interested in the multicast information addressed to that group.

Upon receiving an IGMP report, the switch forwards it through all the router ports in the VLAN, resolves the address of the multicast group the host is interested in, and performs the following to the receiving port:

- If the port is already in the forwarding table, the switch resets the member port aging timer of the port.
- If the port is not in the forwarding table, the switch installs an entry for this port in the forwarding table and starts the member port aging timer of this port.

Note

A switch will not forward an IGMP report through a non-router port for the following reason: Due to the IGMP report suppression mechanism, if member hosts of that multicast group still exist under non-router ports, the hosts will stop sending reports when they receive the message, and this prevents the switch from knowing if members of that multicast group are still attached to these ports.

When receiving a leave message

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave message, so the switch cannot know immediately that the host has left the multicast group. However, as the host stops sending IGMP reports as soon as it leaves a multicast group, the switch deletes the forwarding entry for the member port corresponding to the host from the forwarding table when its aging timer expires.

When an IGMPv2 or IGMPv3 host leaves a multicast group, the host sends an IGMP leave message to the multicast router to announce that it has leaf the multicast group.

Upon receiving an IGMP leave message on the last member port, a switch forwards it out all router ports in the VLAN. Because the switch does not know whether any other member hosts of that multicast group still exists under the port to which the IGMP leave message arrived, the switch does not immediately delete the forwarding entry corresponding to that port from the forwarding table; instead, it resets the aging timer of the member port.

Upon receiving the IGMP leave message from a host, the IGMP querier resolves from the message the address of the multicast group that the host just left and sends an IGMP group-specific query to that multicast group through the port that received the leave message. Upon receiving the IGMP group-specific query, a switch forwards it through all the router ports in the VLAN and all member ports of that multicast group, and performs the following to the receiving port:

- If any IGMP report in response to the group-specific query arrives to the member port before its aging timer expires, this means that some other members of that multicast group still exist under that port: the switch resets the aging timer of the member port.
- If no IGMP report in response to the group-specific query arrives to the member port before its aging timer expires as a response to the IGMP group-specific query, this means that no members of that multicast group still exist under the port: the switch deletes the forwarding entry corresponding to the port from the forwarding table when the aging timer expires.

Caution

After an Ethernet switch enables IGMP Snooping, when it receives the IGMP leave message sent by a host in a multicast group, it judges whether the multicast group exists automatically. If the multicast group does not exist, the switch drops this IGMP leave message.

Configuring IGMP Snooping

Complete the following tasks to configure IGMP Snooping:

Task	Remarks
Enabling IGMP Snooping	Required
Configuring the Version of IGMP Snooping	Optional
Configuring Timers	Optional
Configuring Fast Leave Processing	Optional
Configuring a Multicast Group Filter	Optional
Configuring the Maximum Number of Multicast Groups on a Port	Optional
Configuring IGMP Snooping Querier	Optional
Suppressing Flooding of Unknown Multicast Traffic in a VLAN	Optional
Configuring Static Member Port for a Multicast Group	Optional
Configuring a Static Router Port	Optional
Configuring a Port as a Simulated Group Member	Optional
Configuring a VLAN Tag for Query Message	Optional
Configuring Multicast VLAN	Optional

Enabling IGMP Snooping

Follow these steps to enable IGMP Snooping:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable IGMP Snooping globally	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled globally.
Enter VLAN view	**vlan** *vlan-id*	—
Enable IGMP Snooping on the VLAN	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled on all the VLANs.

Caution

- Although both Layer 2 and Layer 3 multicast protocols can run on the same switch simultaneously, they cannot run simultaneously on a VLAN or its corresponding VLAN interface.
- Before enabling IGMP Snooping in a VLAN, be sure to enable IGMP Snooping globally in system view; otherwise the IGMP Snooping settings will not take effect.
- If IGMP Snooping and VLAN VPN are enabled on a VLAN at the same time, IGMP queries are likely to fail to pass the VLAN. You can solve this problem by configuring VLAN tags for queries. For details, see Configuring a VLAN Tag for Query Messages.

Configuring the Version of IGMP Snooping

With the development of multicast technologies, IGMPv3 has found increasingly wide application. In IGMPv3, a host can not only join a specific multicast group but also explicitly specify to receive or reject the information from a specific multicast source. Working with PIM-SSM, IGMPv3 enables hosts to join specific multicast sources and groups directly, greatly simplifying multicast routing protocols and optimizing the network topology.

By configuring an IGMP snooping version, you actually configure the version of IGMP messages that IGMP snooping can process.

- IGMP snooping version 2 can process IGMPv1 and IGMPv2 messages, but not IGMPv3 messages, which will be flooded in the VLAN.
- IGMP snooping version 3 can process IGMPv1, IGMPv2 and IGMPv3 messages.

Follow these steps to configure the version of IGMP Snooping:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Configure the version of IGMP Snooping	**igmp-snooping version** *version-number*	Optional The default IGMP Snooping version is version 2.

Caution

- Before configuring related IGMP Snooping functions, you must enable IGMP Snooping in the specified VLAN.
- Different multicast group addresses should be configured for different multicast sources because IGMPv3 Snooping cannot distinguish multicast data from different sources to the same multicast group.

Configuring Timers

This section describes how to configure the aging timer of the router port, the aging timer of the multicast member ports, and the query response timer.

Follow these steps to configure timers:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the aging timer of the router port	**igmp-snooping router-aging-time** *seconds*	Optional By default, the aging time of the router port is 105 seconds.
Configure the general query response timer	**igmp-snooping max-response-time** *seconds*	Optional By default, the general query response timeout time is 10 seconds.
Configure the aging timer of the multicast member port	**igmp-snooping host-aging-time** *seconds*	Optional By default, the aging time of multicast member ports is 260 seconds

Configuring Fast Leave Processing

With fast leave processing enabled, when the switch receives an IGMP leave message on a port, the switch directly removes that port from the forwarding table entry for the specific group. If only one host is attached to the port, enable fast leave processing to improve bandwidth management.

If only one host is attached to the port, enable fast leave processing helps improve bandwidth and resource usage. If fast leave processing and unknown multicast packet dropping or non-flooding are enabled on a port to which more than one host is connected, when one host leaves a multicast group, the other hosts connected to port and interested in the same multicast group will fail to receive multicast data for that group.

Enabling fast leave processing in system view

Follow these steps to enable fast leave processing in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable fast leave processing	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Required By default, the fast leave processing feature is disabled.

Enabling fast leave processing in Ethernet port view

Follow these steps to enable fast leave processing in Ethernet view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—

To do...	Use the command...	Remarks
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable fast leave processing for specific VLANs	**igmp-snooping fast-leave** [**vlan** *vlan-list*]	Required By default, the fast leave processing feature is disabled.

Note

- The fast leave processing function works for a port only if the host attached to the port runs IGMPv2 or IGMPv3.
- The configuration performed in system view takes effect on all ports of the switch if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).
- The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).

Configuring a Multicast Group Filter

On an IGMP Snooping-enabled switch, the configuration of a multicast group allows the service provider to define restrictions on multicast programs available to different users.

In an actual application, when a user requests a multicast program, the user's host initiates an IGMP report. Upon receiving this report message, the switch checks the report against the ACL rule configured on the receiving port. If the receiving port can join this multicast group, the switch adds this port to the IGMP Snooping multicast group list; otherwise the switch drops this report message. Any multicast data that has failed the ACL check will not be sent to this port. In this way, the service provider can control the VOD programs provided for multicast users.

Make sure that an ACL rule has been configured before configuring this feature.

Configuring a multicast group filter in system view

Follow these steps to configure a multicast group filter in system view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure a multicast group filter	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Required No group filter is configured by default, namely hosts can join any multicast group.

Configuring a multicast group filter in Ethernet port view

Follow these steps to configure a multicast group filter in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure a multicast group filter	**igmp-snooping group-policy** *acl-number* [**vlan** *vlan-list*]	Optional No group filter is configured by default, namely hosts can join any multicast group.

Note

- A port can belong to multiple VLANs, you can configure only one ACL rule per VLAN on a port.
- If no ACL rule is configured, all the multicast groups will be filtered.
- Since most devices broadcast unknown multicast packets by default, this function is often used together with the function of dropping unknown multicast packets to prevent multicast streams from being broadcast as unknown multicast packets to a port blocked by this function.
- The configuration performed in system view takes effect on all ports of the switch if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on all ports in the specified VLAN(s).
- The configuration performed in Ethernet port view takes effect on the port no matter which VLAN it belongs to if no VLAN is specified; if one or more VLANs are specified, the configuration takes effect on the port only if the port belongs to the specified VLAN(s).

Configuring the Maximum Number of Multicast Groups on a Port

By configuring the maximum number of multicast groups that can be joined on a port, you can limit the number of multicast programs on-demand available to users, thus to regulate traffic on the port.

Follow these steps to configure the maximum number of multicast groups on a port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Limit the number of multicast groups on a port	**igmp-snooping group-limit** *limit* [**vlan** *vlan-list* [**overflow-replace**]]	Required The maximum number of multicast groups on a port is 256 by default.

Note

- To prevent bursting traffic in the network or performance deterioration of the device caused by excessive multicast groups, you can set the maximum number of multicast groups that the switch should process.
- When the number of multicast groups exceeds the configured limit, the switch removes its multicast forwarding entries starting from the oldest one. In this case, the multicast packets for the removed multicast group(s) will be flooded in the VLAN as unknown multicast packets. As a result, non-member ports can receive multicast packets within a period of time. To avoid this from happening, enable the function of dropping unknown multicast packets.

Configuring IGMP Snooping Querier

In an IP multicast network running IGMP, one dedicated multicast device is responsible for sending IGMP general queries, and this router or Layer 3 switch is called the IGMP querier.

However, a Layer 2 multicast switch does not support IGMP, and therefore cannot send general queries by default. By enabling IGMP Snooping querier on a Layer 2 switch in a VLAN where multicast traffic needs to be Layer-2 switched only and no multicast routers are present, the Layer 2 switch will act as a querier to send IGMP general queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

Upon receiving an IGMP query with the source IP address 0.0.0.0 on a port, the switch does not enlist that port as a dynamic router port. This may prevent multicast forwarding entries from being correctly created at the data link layer and cause multicast traffic forwarding failure in the end. When a Layer 2 device acts as an IGMP-Snooping querier, to avoid the aforesaid problem, configure a non-all-zero IP address as the source IP address of IGMP queries.

IGMP Snooping querier related configurations include:

- Enabling IGMP Snooping querier,
- Configuring the IGMP query interval, and
- Configuring the source address to be carried in IGMP general and group specific queries.

Enabling IGMP Snooping querier

Follow these steps to enable IGMP Snooping querier:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable IGMP Snooping	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled.
Enter VLAN view	**vlan** *vlan-id*	—
Enable IGMP Snooping	**igmp-snooping enable**	Required By default, IGMP Snooping is disabled.

To do...	Use the command...	Remarks
Enable IGMP Snooping querier	**igmp-snooping querier**	Required By default, IGMP Snooping querier is disabled.

Configuring IGMP query interval

Follow these steps to configure IGMP query interval:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Configure the IGMP query interval	**igmp-snooping query-interval** *seconds*	Optional 60 seconds by default.

Configuring the source address to be carried in IGMP queries

Follow these steps to configure the source address to be carried in IGMP queries:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Configure the source IP address of IGMP general queries	**igmp-snooping general-query source-ip** { **current-interface** | *ip-address* }	Optional 0.0.0.0 by default

Suppressing Flooding of Unknown Multicast Traffic in a VLAN

With IGMP Snooping enabled in a VLAN, multicast traffic for unknown multicast groups is flooded within the VLAN by default. This wastes network bandwidth and affects multicast forwarding efficiency.

With the unknown multicast flooding suppression function enabled, when receiving a multicast packet for an unknown multicast group, an IGMP Snooping switch creates a nonflooding entry and relays the packet to router ports only, instead of flooding the packet within the VLAN. If the switch has no router ports, it drops the multicast packet.

Follow these steps to suppress flooding of unknown multicast traffic in the VLAN:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable unknown multicast flooding suppression	**igmp-snooping nonflooding-enable**	Required By default, unknown multicast flooding suppression

Note

- If the function of dropping unknown multicast packets or the XRN fabric function is enabled, you cannot enable unknown multicast flooding suppression.
- Unknown multicast flooding suppression and multicast source port suppression cannot take effect at the same time. If both are enabled, only multicast source port suppression takes effect. In this case, multicast data received on the blocked port will be dropped.

Configuring Static Member Port for a Multicast Group

If the host connected to a port is interested in the multicast data for a specific group, you can configure that port as a static member port for that multicast group.

In Ethernet port view

Follow these steps to configure a static multicast group member port in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the current port as a static member port for a multicast group in a VLAN	**multicast static-group** *group-address* **vlan** *vlan-id*	Required By default, no port is configured as a static multicast group member port.

In VLAN interface view

Follow these steps to configure a static multicast group member port in VLAN interface view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface vlan-interface** *interface-number*	—
Configure specified port(s) as static member port(s) of a multicast group in the VLAN	**multicast static-group** *group-address* **interface** *interface-list*	Required By default, no port is configured as a static multicast group member port.

Caution

- You can configure up to 200 static member ports on an Switch 4500 series switch.
- If a port has been configured as an XRN fabric port or a reflect port, it cannot be configured as a static member port.

Configuring a Static Router Port

In a network where the topology is unlikely to change, you can configure a port on the switch as a static router port, so that the switch has a static connection to a multicast router and receives IGMP messages from that router.

In Ethernet port view

Follow these steps to configure a static router port in Ethernet port view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the current port as a static router port	**multicast static-router-port vlan** *vlan-id*	Required By default, no static router port is configured.

In VLAN view

Follow these steps to configure a static router port in VLAN view:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter VLAN view	**vlan** *vlan-id*	—
Configure a specified port as a static router port	**multicast static-router-port** *interface-type interface-number*	Required By default, no static router port is configured.

Configuring a Port as a Simulated Group Member

Generally, hosts running IGMP respond to the IGMP query messages of the multicast switch. If hosts fail to respond for some reason, the multicast switch may consider that there is no member of the multicast group on the local subnet and remove the corresponding path.

To avoid this from happening, you can configure a port of the VLAN of the switch as a multicast group member. When the port receives IGMP query messages, the multicast switch will respond. As a result, the port of the VLAN can continue to receive multicast traffic.

Through this configuration, the following functions can be implemented:

- When an Ethernet port is configured as a simulated member host, the switch sends an IGMP report through this port. Meanwhile, the switch sends the same IGMP report to itself and establishes a corresponding IGMP entry based on this report.
- When receiving an IGMP general query, the simulated host responds with an IGMP report. Meanwhile, the switch sends the same IGMP report to itself to ensure that the IGMP entry does not age out.
- When the simulated joining function is disabled on an Ethernet port, the simulated host sends an IGMP leave message.

Therefore, to ensure that IGMP entries will not age out, the port must receive IGMP general queries periodically.

Follow these steps to configure a port as a simulated group member:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the current port as a simulated multicast group member	**igmp host-join** *group-address* [**source-ip** *source-address*] **vlan** *vlan-id*	Required Simulated joining is disabled by default.

Caution

- Before configuring a simulated host, enable IGMP Snooping in VLAN view first.
- The port to be configured must belong to the specified VLAN; otherwise the configuration does not take effect.
- You can use the source-ip source-address command to specify a multicast source address that the port will join as a simulated host. This configuration takes effect when IGMPv3 Snooping is enabled in the VLAN.

Configuring a VLAN Tag for Query Messages

By configuring the VLAN tag carried in IGMP general and group-specific queries forwarded and sent by IGMP Snooping switches, you can enable multicast packet forwarding between different VLANs In a Layer-2 multicast network environment.

Follow these steps to configure VLAN tag for query message:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure a VLAN tag for query messages	**igmp-snooping vlan-mapping vlan** *vlan-id*	Required By default, the VLAN tag in IGMP general and group-specific query messages is not changed.

Note

It is not recommended to configure this function while the multicast VLAN function is in effect.

Configuring Multicast VLAN

In traditional multicast implementations, when users in different VLANs listen to the same multicast group, the multicast data is copied on the multicast router for each VLAN that contains receivers. This is a big waste of network bandwidth.

In an IGMP Snooping environment, by configuring a multicast VLAN and adding ports to the multicast VLAN, you can allow users in different VLANs to share the same multicast VLAN. This saves bandwidth because multicast streams are transmitted only within the multicast VLAN. In addition, because the multicast VLAN is isolated from user VLANs, this method also enhances the information security.

Multicast VLAN is mainly used in Layer 2 switching, but you must make the corresponding configurations on the Layer 3 switch.

Follow these steps to configure multicast VLAN on the Layer 3 switch:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create a multicast VLAN and enter VLAN view	**vlan** *vlan-id*	—
Return to system view	**quit**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Enable IGMP	**igmp enable**	Required By default, the IGMP feature is disabled.
Return to system view	**quit**	—
Enter Ethernet port view for the Layer 2 switch to be configured	**interface** *interface-type interface-number*	—
Define the port as a trunk or hybrid port	**port link-type** { **trunk** | **hybrid** }	Required
Specify the VLANs to be allowed to pass the Ethernet port	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required The multicast VLAN defined on the Layer 2 switch must be included, and the port must be configured to forward tagged packets for the multicast VLAN if the port type is hybrid.
	port trunk permit vlan *vlan-list*	

Follow these steps to configure multicast VLAN on the Layer 2 switch:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable IGMP Snooping	**igmp-snooping enable**	—
Enter VLAN view	**vlan** *vlan-id*	—
Enable IGMP Snooping	**igmp-snooping enable**	Required
Enable multicast VLAN	**service-type multicast**	Required
Return to system view	**quit**	—

To do...	Use the command...	Remarks
Enter Ethernet port view for the Layer 3 switch	**interface** *interface-type interface-number*	—
Define the port as a trunk or hybrid port	**port link-type** { **trunk** | **hybrid** }	Required
Specify the VLANs to be allowed to pass the Ethernet port	**port hybrid vlan** *vlan-list* { **tagged** | **untagged** }	Required The multicast VLAN must be included, and the port must be configured to forward tagged packets for the multicast VLAN if the port type is hybrid.
	port trunk permit vlan *vlan-list*	
Enter Ethernet port view for a user device	**interface** *interface-type interface-number*	—
Define the port as a hybrid port	**port link-type hybrid**	Required
Specify the VLANs to be allowed to pass the port	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	Required The multicast VLAN must be included, and the port must be configured to forward tagged packets for the multicast VLAN.

Note

- One port can belong to only one multicast VLAN.
- The port connected to a user terminal must be a hybrid port.
- The multicast member ports must be in the same VLAN with the router port. Otherwise, the multicast member port cannot receive multicast packets.
- If a router port is in a multicast VLAN, the router port must be configured as a trunk port or a hybrid port that allows tagged packets to pass for the multicast VLAN. Otherwise, all the multicast member ports in this multicast VLAN cannot receive multicast packets.
- The multicast VLAN function and the VLAN mapping function cannot be configured at the same time.

Displaying and Maintaining IGMP Snooping

To do...	Use the command…	Remarks
Display the current IGMP Snooping configuration	**display igmp-snooping configuration**	Available in any view
Display IGMP Snooping message statistics	**display igmp-snooping statistics**	Available in any view
Display the information about IP and MAC multicast groups in one or all VLANs	**display igmp-snooping group** [**vlan** *vlan-id*]	Available in any view
Clear IGMP Snooping statistics	**reset igmp-snooping statistics**	Available in user view

IGMP Snooping Configuration Examples

Configuring IGMP Snooping

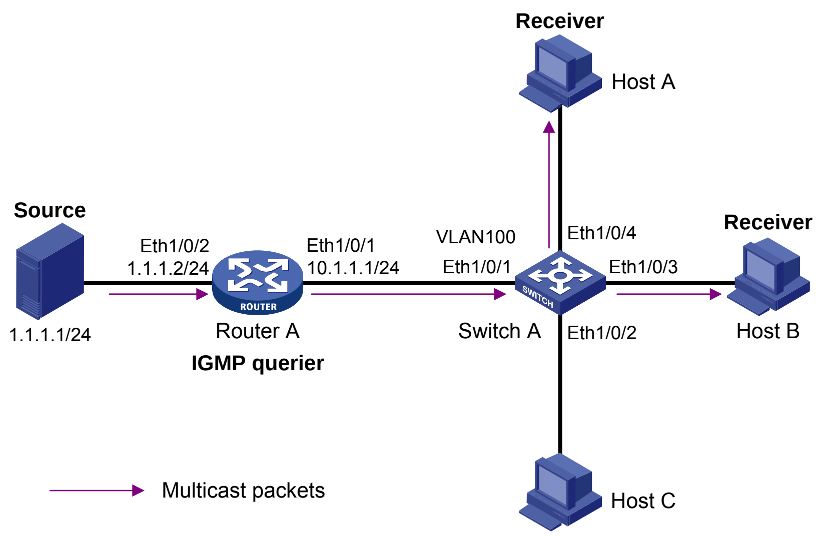
Network requirements

To prevent multicast traffic from being flooded at Layer 2, enable IGMP snooping on Layer 2 switches.

- As shown in Figure 3-3, Router A connects to a multicast source (Source) through Ethernet 1/0/2, and to Switch A through Ethernet 1/0/1.
- Run PIM-DM and IGMP on Router A. Run IGMP snooping on Switch A. Router A acts as the IGMP querier.
- The multicast source sends multicast data to the multicast group 224.1.1.1. Host A and Host B are receivers of the multicast group 224.1.1.1.

Network diagram

Figure 3-3 Network diagram for IGMP Snooping configuration



Configuration procedure

1) Configure the IP address of each interface

Configure an IP address and subnet mask for each interface as per Figure 3-3. The detailed configuration steps are omitted.

2) Configure Router A

Enable IP multicast routing, enable PIM-DM on each interface, and enable IGMP on Ethernet 1/0/1.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface Ethernet 1/0/1
[RouterA-Ethernet1/0/1] igmp enable
[RouterA-Ethernet1/0/1] pim dm
[RouterA-Ethernet1/0/1] quit
[RouterA] interface Ethernet 1/0/2
[RouterA-Ethernet1/0/2] pim dm
[RouterA-Ethernet1/0/2] quit
```

3) Configure Switch A

Enable IGMP Snooping globally.

```
<SwitchA> system-view
[SwitchA] igmp-snooping enable
  Enable IGMP-Snooping ok.
```

Create VLAN 100, assign Ethernet 1/0/1 through Ethernet 1/0/4 to this VLAN, and enable IGMP Snooping in the VLAN.

```
[SwitchA] vlan 100
[SwitchA-vlan100] port Ethernet 1/0/1 to Ethernet 1/0/4
[SwitchA-vlan100] igmp-snooping enable
[SwitchA-vlan100] quit
```

4) Verify the configuration

View the detailed information of the multicast group in VLAN 100 on Switch A.

```
<SwitchA> display igmp-snooping group vlan100
  Total 1 IP Group(s).
  Total 1 MAC Group(s).

  Vlan(id):100.
    Total 1 IP Group(s).
    Total 1 MAC Group(s).
    Static Router port(s):
    Dynamic Router port(s):
                     Ethernet1/0/1
    IP group(s):the following ip group(s) match to one mac group.
        IP group address: 224.1.1.1
        Static host port(s):
        Dynamic host port(s):
                     Ethernet1/0/3          Ethernet1/0/4
    MAC group(s):
        MAC group address: 0100-5e01-0101
        Host port(s): Ethernet1/0/3          Ethernet1/0/4
```

As shown above, the multicast group 224.1.1.1 has been registered on Switch A, with the dynamic router port Ethernet 1/0/1 and dynamic member ports Ethernet 1/0/3 and Ethernet 1/0/4. This means that Host A and Host B have joined the multicast group 224.1.1.1.

Configuring Multicast VLAN

Network requirements

As shown in Figure 3-4, Workstation is a multicast source. Switch A forwards multicast data from the multicast source. A Layer 2 switch, Switch B forwards the multicast data to the end users Host A and Host B.

Table 3-2 describes the network devices involved in this example and the configurations you should make on them.

Table 3-2 Network devices and their configurations

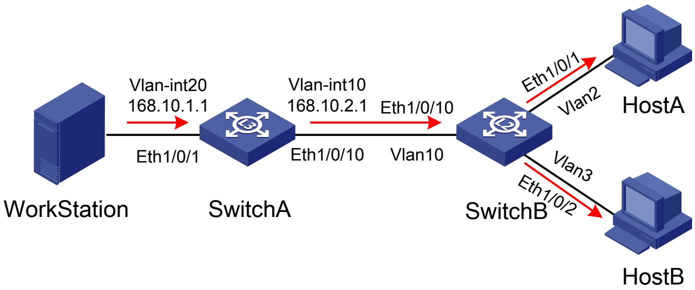
Device	Device description	Networking description
Switch A	Layer 3 switch	The interface IP address of VLAN 20 is 168.10.1.1. Ethernet 1/0/1 is connected to the workstation and belongs to VLAN 20. The interface IP address of VLAN 10 is 168.10.2.1. Ethernet 1/0/10 belongs to VLAN 10. Ethernet 1/0/10 is connected to Switch B.
Switch B	Layer 2 switch	• VLAN 2 contains Ethernet 1/0/1 and VLAN 3 contains Ethernet 1/0/2. • The default VLANs of Ethernet 1/0/1 and Ethernet 1/0/2 are VLAN 2 and VLAN 3 respectively. • VLAN 10 contains Ethernet 1/0/10, Ethernet 1/0/1, and Ethernet 1/0/2. Ethernet 1/0/10 is connected to Switch A. • VLAN 10 is a multicast VLAN. • Ethernet 1/0/1 sends untagged packets for VLAN 2 and VLAN 10. • Ethernet 1/0/2 sends untagged packets for VLAN 3 and VLAN 10.
Host A	User 1	Host A is connected to Ethernet 1/0/1 on Switch B.
Host B	User 2	Host B is connected to Ethernet 1/0/2 on Switch B.

In this configuration example, you need to configure the ports that connect Switch A and Switch B to each other as hybrid ports. The following text describes the configuration details. You can also configure these ports as trunk ports. The configuration procedure is omitted here. For details, see Configuring Multicast VLAN.

Configure a multicast VLAN, so that users in VLAN 2 and VLAN 3 can receive multicast streams through the multicast VLAN.

Network diagram

Figure 3-4 Network diagram for multicast VLAN configuration



Configuration procedure

The following configuration is based on the prerequisite that the devices are properly connected and all the required IP addresses are already configured.

1) Configure Switch A:

Set the interface IP address of VLAN 20 to 168.10.1.1 and enable PIM DM on the VLAN interface.

```
<SwitchA> system-view
[SwitchA] multicast routing-enable
[SwitchA] vlan 20
[SwitchA–vlan20]port Ethernet 1/0/1
[SwitchA-vlan20] quit
[SwitchA] interface Vlan-interface 20
[SwitchA-Vlan-interface20] ip address 168.10.1.1 255.255.255.0
[SwitchA-Vlan-interface20] pim dm
[SwitchA-Vlan-interface20] quit
```

Configure VLAN 10.

```
[SwitchA] vlan 10
[SwitchA-vlan10] quit
```

Define Ethernet 1/0/10 as a hybrid port, add the port to VLAN 10, and configure the port to forward tagged packets for VLAN 10.

```
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] port link-type hybrid
[SwitchA-Ethernet1/0/10] port hybrid vlan 10 tagged
[SwitchA-Ethernet1/0/10] quit
```

Configure the interface IP address of VLAN 10 as 168.10.2.1, and enable PIM-DM and IGMP.

```
[SwitchA] interface Vlan-interface 10
[SwitchA-Vlan-interface10] ip address 168.10.2.1 255.255.255.0
[SwitchA-Vlan-interface10] igmp enable
[SwitchA-Vlan-interface10] pim dm
```

2) Configure Switch B:

Enable the IGMP Snooping feature on Switch B.

```
<SwitchB> system-view
[SwitchB] igmp-snooping enable
```

Create VLAN 2, VLAN 3 and VLAN 10, configure VLAN 10 as the multicast VLAN, and then enable IGMP Snooping on it.

```
[SwitchB] vlan 2 to 3
Please wait.... Done.
[SwitchB] vlan 10
[SwitchB-vlan10] service-type multicast
[SwitchB-vlan10] igmp-snooping enable
[SwitchB-vlan10] quit
```

Define Ethernet 1/0/10 as a hybrid port, add the port to VLAN 2, VLAN 3, and VLAN 10, and configure the port to forward tagged packets for VLAN 2, VLAN 3, and VLAN 10.

```
[SwitchB] interface Ethernet 1/0/10
[SwitchB-Ethernet1/0/10] port link-type hybrid
[SwitchB-Ethernet1/0/10] port hybrid vlan 2 3 10 tagged
[SwitchB-Ethernet1/0/10] quit
```

Define Ethernet 1/0/1 as a hybrid port, add the port to VLAN 2 and VLAN 10, configure the port to forward untagged packets for VLAN 2 and VLAN 10, and set VLAN 2 as the default VLAN of the port.

```
[SwitchB] interface Ethernet 1/0/1
[SwitchB-Ethernet1/0/1] port link-type hybrid
[SwitchB-Ethernet1/0/1] port hybrid vlan 2 10 untagged
[SwitchB-Ethernet1/0/1] port hybrid pvid vlan 2
[SwitchB-Ethernet1/0/1] quit
```

Define Ethernet 1/0/2 as a hybrid port, add the port to VLAN 3 and VLAN 10, configure the port to forward untagged packets for VLAN 3 and VLAN 10, and set VLAN 3 as the default VLAN of the port.

```
[SwitchB] interface Ethernet 1/0/2
[SwitchB-Ethernet1/0/2] port link-type hybrid
[SwitchB-Ethernet1/0/2] port hybrid vlan 3 10 untagged
[SwitchB-Ethernet1/0/2] port hybrid pvid vlan 3
[SwitchB-Ethernet1/0/2] quit
```

Troubleshooting IGMP Snooping

Symptom: Multicast function does not work on the switch.

Solution:

Possible reasons are:

1) IGMP Snooping is not enabled.

- Use the **display current-configuration** command to check the status of IGMP Snooping.
- If IGMP Snooping is disabled, check whether it is disabled globally or in the specific VLAN. If it is disabled globally, use the **igmp-snooping enable** command in both system view and VLAN view to enable it both globally and on the corresponding VLAN at the same time. If it is only disabled on the corresponding VLAN, use the **igmp-snooping enable** command in VLAN view only to enable it on the corresponding VLAN.

2) Multicast forwarding table set up by IGMP Snooping is wrong.

- Use the **display igmp-snooping group** command to check if the multicast groups are expected ones.

- If the multicast group set up by IGMP Snooping is not correct, contact your technical support personnel.

Table of Contents

1 802.1x Configuration

When configuring 802.1x, go to these sections for information you are interested in:

- Introduction to 802.1x
- Introduction to 802.1x Configuration
- Basic 802.1x Configuration
- Advanced 802.1x Configuration
- Displaying and Maintaining 802.1x Configuration
- Configuration Example

Introduction to 802.1x

The 802.1x protocol (802.1x for short) was developed by IEEE802 LAN/WAN committee to address security issues of wireless LANs. It was then used in Ethernet as a common access control mechanism for LAN ports to address mainly authentication and security problems.

802.1x is a port-based network access control protocol. It is used to perform port-level authentication and control of devices connected to the 802.1x-enabled ports. With the 802.1x protocol employed, a user-side device can access the LAN only when it passes the authentication. Those devices that fail to pass the authentication are denied access to the LAN.

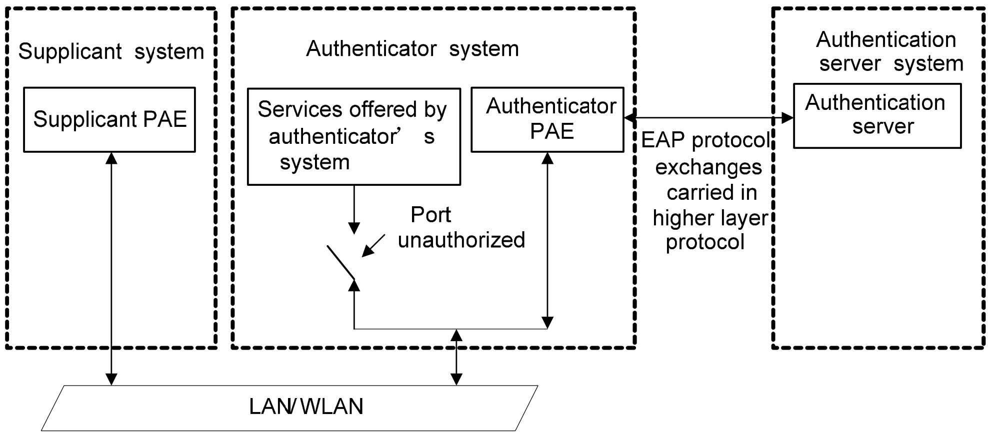
This section covers these topics:

- Architecture of 802.1x Authentication
- The Mechanism of an 802.1x Authentication System
- Encapsulation of EAPoL Messages
- 802.1x Authentication Procedure
- Timers Used in 802.1x
- Additional 802.1x Features on Switch

Architecture of 802.1x Authentication

As shown in Figure 1-1, 802.1x adopts a client/server architecture with three entities: a supplicant system, an authenticator system, and an authentication server system.

Figure 1-1 Architecture of 802.1x authentication



- The supplicant system is the entity seeking access to the LAN. It resides at one end of a LAN segment and is authenticated by the authenticator system at the other end of the LAN segment. The supplicant system is usually a user terminal device. An 802.1x authentication is triggered when a user launches an 802.1x-capable client program on the supplicant system. Note that the client program must support the extensible authentication protocol over LAN (EAPoL).
- The authenticator system, residing at the other end of the LAN segment, is the entity that authenticates the connected supplicant system. The authenticator system is usually an 802.1x-supported network device, such as an H3C series switch. It provides the port (physical or logical) for the supplicant system to access the LAN.
- The authentication server system is the entity that provides authentication services to the authenticator system. The authentication server system, usually a RADIUS server, serves to perform Authentication, Authorization, and Accounting (AAA) services to users. It also stores user information, such as user name, password, the VLAN a user should belong to, priority, and any Access Control Lists (ACLs) to be applied.

There are four additional basic concepts related 802.1x: port access entity (PAE), controlled port and uncontrolled port, the valid direction of a controlled port and the access control method on ports.

I. PAE

A port access entity (PAE) is responsible for implementing algorithms and performing protocol-related operations in the authentication mechanism.

- The authenticator system PAE authenticates the supplicant systems when they log into the LAN and controls the status (authorized/unauthorized) of the controlled ports according to the authentication result.
- The supplicant system PAE responds to the authentication requests received from the authenticator system and submits user authentication information to the authenticator system. It also sends authentication requests and disconnection requests to the authenticator system PAE.

Controlled port and uncontrolled port

The authenticator system provides ports for supplicant systems to access a LAN. Logically, a port of this kind is divided into a controlled port and an uncontrolled port.

- The uncontrolled port can always send and receive packets. It mainly serves to forward EAPoL packets to ensure that a supplicant system can send and receive authentication requests.

- The controlled port can be used to pass service packets when it is in authorized state. It is blocked when not in authorized state. In this case, no packets can pass through it.
- Controlled port and uncontrolled port are two properties of a port. Packets reaching a port are visible to both the controlled port and uncontrolled port of the port.

The valid direction of a controlled port

When a controlled port is in unauthorized state, you can configure it to be a unidirectional port, which sends packets to supplicant systems only.

By default, a controlled port is a unidirectional port.

The way a port is controlled

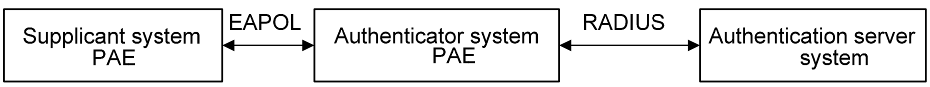
A port of an H3C series switch can be controlled in the following two ways.

- Port-based control. When a port is under port-based control, all the supplicant systems connected to the port can access the network without being authenticated after one supplicant system among them passes the authentication. And when the authenticated supplicant system goes offline, the others are denied as well.
- MAC-based control. When a port is under MAC-based control, all supplicant systems connected to the port have to be authenticated individually in order to access the network. And when a supplicant system goes offline, the others are not affected.

The Mechanism of an 802.1x Authentication System

IEEE 802.1x authentication system uses the Extensible Authentication Protocol (EAP) to exchange information between the supplicant system and the authentication server.

Figure 1-2 The mechanism of an 802.1x authentication system



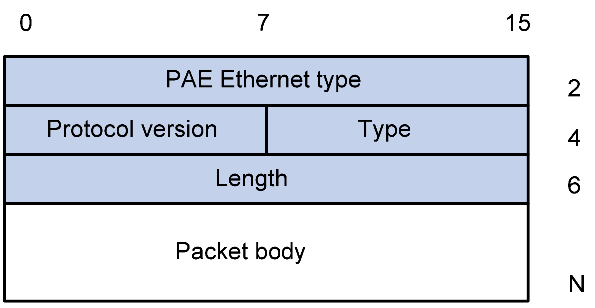
- EAP protocol packets transmitted between the supplicant system PAE and the authenticator system PAE are encapsulated as EAPoL packets.
- EAP protocol packets transmitted between the authenticator system PAE and the RADIUS server can either be encapsulated as EAP over RADIUS (EAPoR) packets or be terminated at system PAEs. The system PAEs then communicate with RADIUS servers through Password Authentication Protocol (PAP) or Challenge-Handshake Authentication Protocol (CHAP) packets.
- When a supplicant system passes the authentication, the authentication server passes the information about the supplicant system to the authenticator system. The authenticator system in turn determines the state (authorized or unauthorized) of the controlled port according to the instructions (accept or reject) received from the RADIUS server.

Encapsulation of EAPoL Messages

The format of an EAPoL packet

EAPoL is a packet encapsulation format defined in 802.1x. To enable EAP protocol packets to be transmitted between supplicant systems and authenticator systems through LANs, EAP protocol packets are encapsulated in EAPoL format. The following figure illustrates the structure of an EAPoL packet.

Figure 1-3 The format of an EAPoL packet



In an EAPoL packet:

- The PAE Ethernet type field holds the protocol identifier. The identifier for 802.1x is 0x888E.
- The Protocol version field holds the version of the protocol supported by the sender of the EAPoL packet.
- The Type field can be one of the following:

    00: Indicates that the packet is an EAP-packet, which carries authentication information.

    01: Indicates that the packet is an EAPoL-start packet, which initiates the authentication.

    02: Indicates that the packet is an EAPoL-logoff packet, which sends logging off requests.

    03: Indicates that the packet is an EAPoL-key packet, which carries key information.

    04: Indicates that the packet is an EAPoL-encapsulated-ASF-Alert packet, which is used to support the alerting messages of Alerting Standards Forum (ASF).

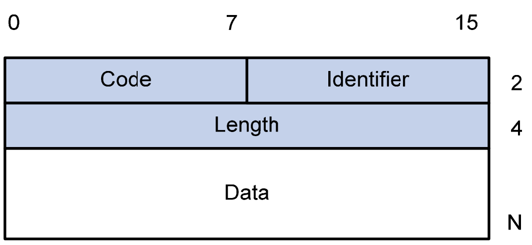
- The Length field indicates the size of the Packet body field. A value of 0 indicates that the Packet Body field does not exist.
- The Packet body field differs with the Type field.

Note that EAPoL-Start, EAPoL-Logoff, and EAPoL-Key packets are only transmitted between the supplicant system and the authenticator system. EAP packets are encapsulated by RADIUS protocol to allow them successfully reach the authentication servers. Network management-related information (such as alarming information) is encapsulated in EAPoL-Encapsulated-ASF-Alert packets, which are terminated by authenticator systems.

The format of an EAP packet

For an EAPoL packet with the value of the Type field being EAP-packet, its Packet body field is an EAP packet, whose format is illustrated in Figure 1-4.

Figure 1-4 The format of an EAP packet



In an EAP packet:

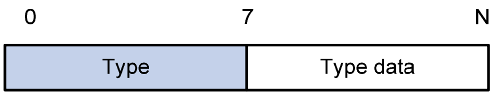
- The Code field indicates the EAP packet type, which can be Request, Response, Success, or Failure.
- The Identifier field is used to match a Response packet with the corresponding Request packet.

- The Length field indicates the size of an EAP packet, which includes the Code, Identifier, Length, and Data fields.
- The Data field carries the EAP packet, whose format differs with the Code field.

A Success or Failure packet does not contain the Data field, so the Length field of it is 4.

Figure 1-5 shows the format of the Data field of a Request packet or a Response packet.

Figure 1-5 The format of the Data field of a Request packet or a Response packet



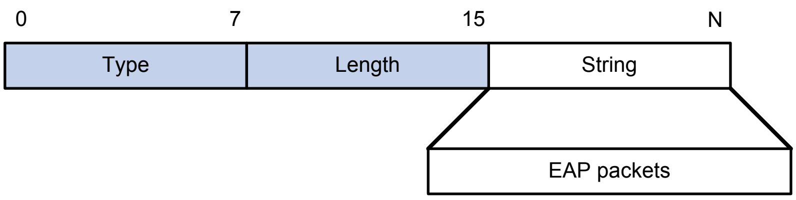
- The Type field indicates the EAP authentication type. A value of 1 indicates Identity and that the packet is used to query the identity of the peer. A value of 4 represents MD5-Challenge (similar to PPP CHAP) and indicates that the packet includes query information.
- The Type Date field differs with types of Request and Response packets.

Fields added for EAP authentication

Two fields, EAP-message and Message-authenticator, are added to a RADIUS protocol packet for EAP authentication. (Refer to the Introduction to RADIUS protocol section in the *AAA Operation* for information about the format of a RADIUS protocol packet.)

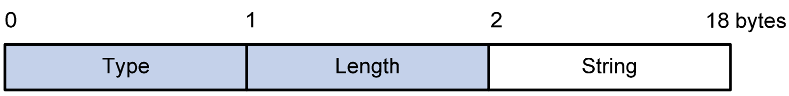
The EAP-message field, whose format is shown in Figure 1-6, is used to encapsulate EAP packets. The maximum size of the string field is 253 bytes. EAP packets with their size larger than 253 bytes are fragmented and are encapsulated in multiple EAP-message fields. The type code of the EAP-message field is 79.

Figure 1-6 The format of an EAP-message field



The Message-authenticator field, whose format is shown in Figure 1-7, is used to prevent unauthorized interception to access requesting packets during authentications using CHAP, EAP, and so on. A packet with the EAP-message field must also have the Message-authenticator field. Otherwise, the packet is regarded as invalid and is discarded.

Figure 1-7 The format of an Message-authenticator field



802.1x Authentication Procedure

Switch 4500 can authenticate supplicant systems in EAP terminating mode or EAP relay mode.

EAP relay mode

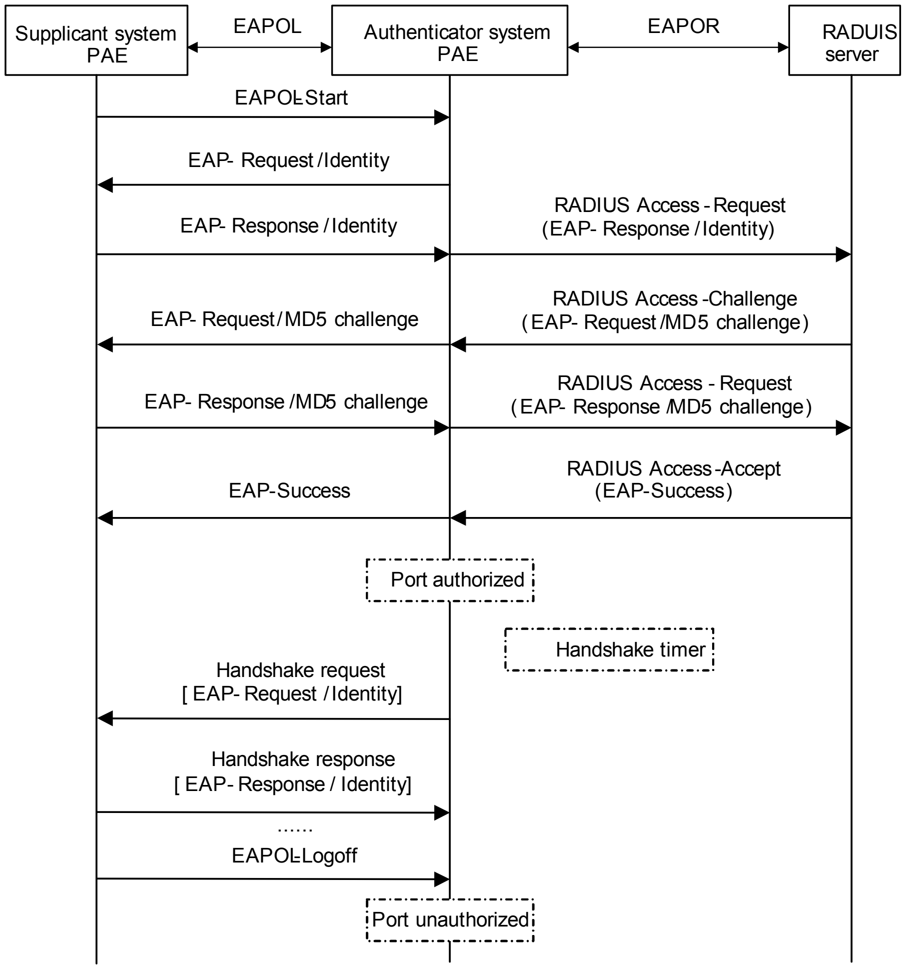
This mode is defined in 802.1x. In this mode, EAP packets are encapsulated in higher level protocol (such as EAPoR) packets to enable them to successfully reach the authentication server. Normally, this mode requires that the RADIUS server support the two newly-added fields: the EAP-message field (with a value of 79) and the Message-authenticator field (with a value of 80).

Four authentication ways, namely EAP-MD5, EAP-TLS (transport layer security), EAP-TTLS (tunneled transport layer security), and Protected Extensible Authentication Protocol (PEAP), are available in the EAP relay mode.

- EAP-MD5 authenticates the supplicant system. The RADIUS server sends MD5 keys (contained in EAP-request/MD5 challenge packets) to the supplicant system, which in turn encrypts the passwords using the MD5 keys.
- EAP-TLS allows the supplicant system and the RADIUS server to check each other's security certificate and authenticate each other's identity, guaranteeing that data is transferred to the right destination and preventing data from being intercepted.
- EAP-TTLS is a kind of extended EAP-TLS. EAP-TLS implements bidirectional authentication between the client and authentication server. EAP-TTLS transmit message using a tunnel established using TLS.
- PEAP creates and uses TLS security channels to ensure data integrity and then performs new EAP negotiations to verify supplicant systems.

Figure 1-8 describes the basic EAP-MD5 authentication procedure.

Figure 1-8 802.1x authentication procedure (in EAP relay mode)



The detailed procedure is as follows:

- A supplicant system launches an 802.1x client to initiate an access request by sending an EAPoL-start packet to the switch, with its user name and password provided. The 802.1x client program then forwards the packet to the switch to start the authentication process.
- Upon receiving the authentication request packet, the switch sends an EAP-request/identity packet to ask the 802.1x client for the user name.
- The 802.1x client responds by sending an EAP-response/identity packet to the switch with the user name contained in it. The switch then encapsulates the packet in a RADIUS Access-Request packet and forwards it to the RADIUS server.
- Upon receiving the packet from the switch, the RADIUS server retrieves the user name from the packet, finds the corresponding password by matching the user name in its database, encrypts the password using a randomly-generated key, and sends the key to the switch through an RADIUS access-challenge packet. The switch then sends the key to the 802.1x client.
- Upon receiving the key (encapsulated in an EAP-request/MD5 challenge packet) from the switch, the client program encrypts the password of the supplicant system with the key and sends the encrypted password (contained in an EAP-response/MD5 challenge packet) to the RADIUS server through the switch. (Normally, the encryption is irreversible.)
- The RADIUS server compares the received encrypted password (contained in a RADIUS access-request packet) with the locally-encrypted password. If the two match, it will then send

feedbacks (through a RADIUS access-accept packet and an EAP-success packet) to the switch to indicate that the supplicant system is authenticated.

- The switch changes the state of the corresponding port to accepted state to allow the supplicant system to access the network.
- The supplicant system can also terminate the authenticated state by sending EAPoL-Logoff packets to the switch. The switch then changes the port state from accepted to rejected.

Note

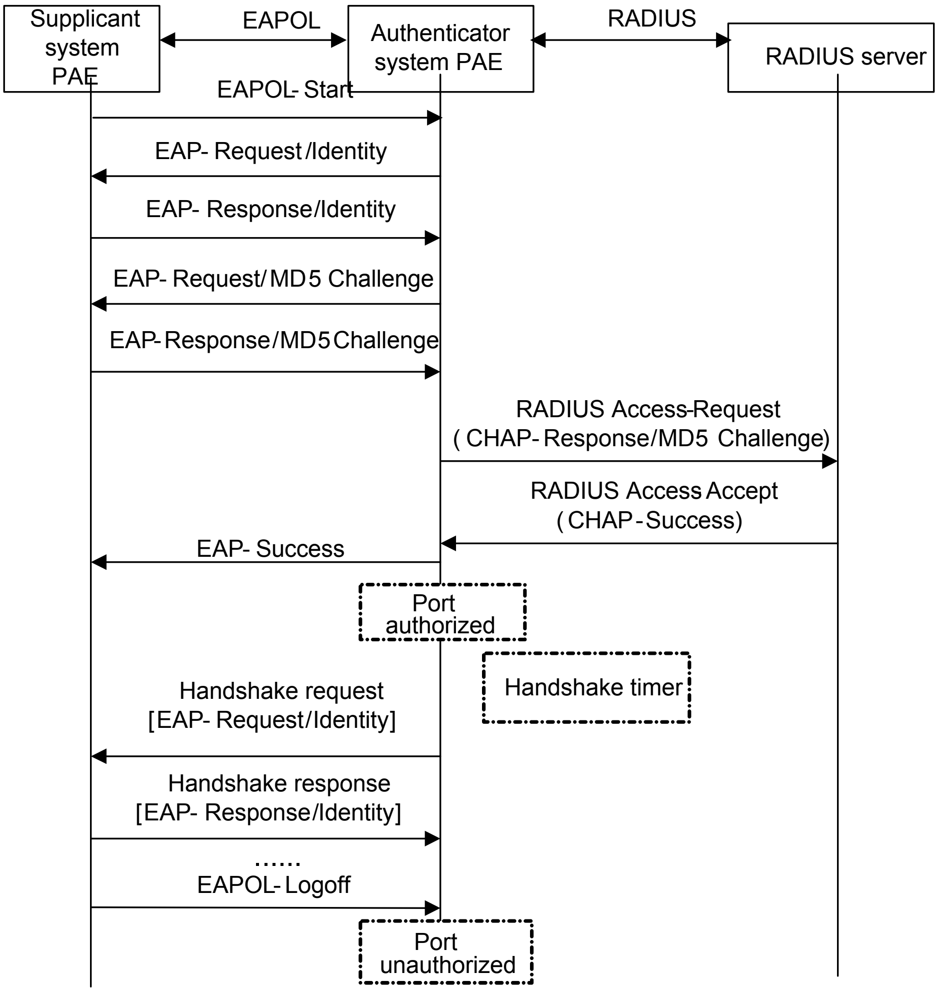
In EAP relay mode, packets are not modified during transmission. Therefore if one of the four ways are used (that is, PEAP, EAP-TLS, EAP-TTLS or EAP-MD5) to authenticate, ensure that the authenticating ways used on the supplicant system and the RADIUS server are the same. However for the switch, you can simply enable the EAP relay mode by using the **dot1x authentication-method eap** command.

EAP terminating mode

In this mode, EAP packet transmission is terminated at authenticator systems and the EAP packets are converted to RADIUS packets. Authentication and accounting are carried out through RADIUS protocol.

In this mode, PAP or CHAP is employed between the switch and the RADIUS server. Figure 1-9 illustrates the authentication procedure (assuming that CHAP is employed between the switch and the RADIUS server).

Figure 1-9 802.1x authentication procedure (in EAP terminating mode)



The authentication procedure in EAP terminating mode is the same as that in the EAP relay mode except that the randomly-generated key in the EAP terminating mode is generated by the switch, and that it is the switch that sends the user name, the randomly-generated key, and the supplicant system-encrypted password to the RADIUS server for further authentication.

Timers Used in 802.1x

In 802.1 x authentication, the following timers are used to ensure that the supplicant system, the switch, and the RADIUS server interact in an orderly way.

- Handshake timer (**handshake-period**). This timer sets the handshake period and is triggered after a supplicant system passes the authentication. It sets the interval for a switch to send handshake request packets to online users. You can set the maximum number of transmission attempts by using the **dot1x retry** command. An online user will be considered offline when the switch has not received any response packets after the maximum number of handshake request transmission attempts is reached.
- Quiet-period timer (**quiet-period**). This timer sets the quiet-period. When a supplicant system fails to pass the authentication, the switch quiets for the set period (set by the quiet-period timer) before it processes another authentication request re-initiated by the supplicant system. During this quiet period, the switch does not perform any 802.1x authentication-related actions for the supplicant system.

- Re-authentication timer (**reauth-period**). The switch initiates 802.1x re-authentication at the interval set by the re-authentication timer.
- RADIUS server timer (**server-timeout**). This timer sets the server-timeout period. After sending an authentication request packet to the RADIUS server, the switch sends another authentication request packet if it does not receive the response from the RADIUS server when this timer times out.
- Supplicant system timer (**supp-timeout**). This timer sets the supp-timeout period and is triggered by the switch after the switch sends a request/challenge packet to a supplicant system. The switch sends another request/challenge packet to the supplicant system if the switch does not receive the response from the supplicant system when this timer times out.
- Transmission timer (**tx-period**). This timer sets the tx-period and is triggered by the switch in two cases. The first case is when the client requests for authentication. The switch sends a unicast request/identity packet to a supplicant system and then triggers the transmission timer. The switch sends another request/identity packet to the supplicant system if it does not receive the reply packet from the supplicant system when this timer times out. The second case is when the switch authenticates the 802.1x client who cannot request for authentication actively. The switch sends multicast request/identity packets periodically through the port enabled with 802.1x function. In this case, this timer sets the interval to send the multicast request/identity packets.
- Client version request timer (**ver-period**). This timer sets the version period and is triggered after a switch sends a version request packet. The switch sends another version request packet if it does receive version response packets from the supplicant system when the timer expires.

Additional 802.1x Features on Switch 4500

In addition to the earlier mentioned 802.1x features, Switch 4500 is also capable of the following:

- Checking supplicant systems for proxies, multiple network adapters, etc. (This function needs the cooperation of a CAMS server.)
- Checking client version
- The guest VLAN function

Note

H3C's CAMS Server is a service management system used to manage networks and to secure networks and user information. With the cooperation of other networking devices (such as switches) in the network, a CAMS server can implement the AAA functions and rights management.

Checking the supplicant system

Switch 4500 checks:

- Supplicant systems logging on through proxies
- Supplicant systems logging on through IE proxies
- Whether or not a supplicant system logs in through more than one network adapters (that is, whether or not more than one network adapters are active in a supplicant system when the supplicant system logs in).

In response to any of the three cases, a switch can optionally take the following measures:

- Only disconnects the supplicant system but sends no Trap packets.
- Sends Trap packets without disconnecting the supplicant system.

This function needs the cooperation of 802.1x client and a CAMS server.

- The 802.1x client needs to be capable of detecting multiple network adapters, proxies, and IE proxies.
- The CAMS server is configured to disable the use of multiple network adapters, proxies, or IE proxies.

By default, an 802.1x client program allows use of multiple network adapters, proxies, and IE proxies. In this case, if the CAMS server is configured to disable use of multiple network adapters, proxies, or IE proxies, it prompts the 802.1x client to disable use of multiple network adapters, proxies, or IE proxies through messages after the supplicant system passes the authentication.

Note

- The client-checking function needs the support of H3C's 802.1x client program.
- To implement the proxy detecting function, you need to enable the function on both the 802.1x client program and the CAMS server in addition to enabling the client version detecting function on the switch by using the **dot1x version-check** command.

Checking the client version

With the 802.1x client version-checking function enabled, a switch checks the version and validity of an 802.1x client to prevent unauthorized users or users with earlier versions of 802.1x client from logging in.

This function makes the switch to send version-requesting packets again if the 802.1x client fails to send version-reply packet to the switch when the version-checking timer times out.

Note

The 802.1x client version-checking function needs the support of H3C's 802.1x client program.

The guest VLAN function

The guest VLAN function enables supplicant systems that are not authenticated to access network resources in a restrained way.

The guest VLAN function enables supplicant systems that do not have 802.1x client installed to access specific network resources. It also enables supplicant systems that are not authenticated to upgrade their 802.1x client programs.

With this function enabled:

- The switch sends authentication triggering request (EAP-Request/Identity) packets to all the 802.1x-enabled ports.

- After the maximum number retries have been made and there are still ports that have not sent any response back, the switch will then add these ports to the guest VLAN.
- Users belonging to the guest VLAN can access the resources of the guest VLAN without being authenticated. But they need to be authenticated when accessing external resources.

Normally, the guest VLAN function is coupled with the dynamic VLAN delivery function.

Refer to *AAA Operation* for detailed information about the dynamic VLAN delivery function.

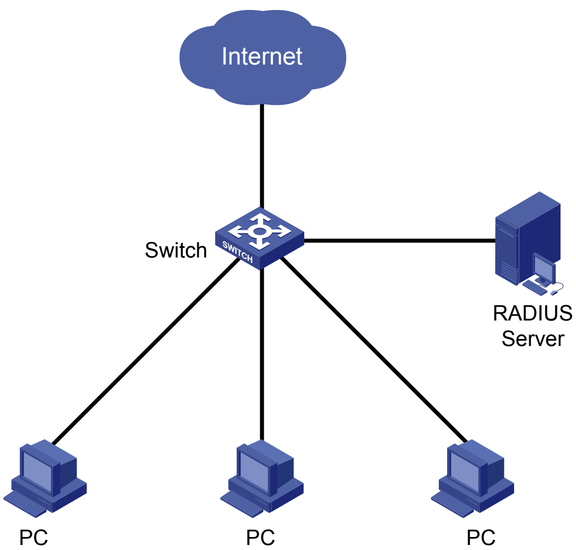
Enabling 802.1x re-authentication

802.1x re-authentication is timer-triggered or packet-triggered. It re-authenticates users who have passed authentication. With 802.1x re-authentication enabled, the switch can monitor the connection status of users periodically. If the switch receives no re-authentication response from a user in a period of time, it tears down the connection to the user. To connect to the switch again, the user needs to initiate 802.1x authentication with the client software again.

Note

- When re-authenticating a user, a switch goes through the complete authentication process. It transmits the username and password of the user to the server. The server may authenticate the username and password, or, however, use re-authentication for only accounting and user connection status checking and therefore does not authenticate the username and password any more.
- An authentication server running CAMS authenticates the username and password during re-authentication of a user in the EAP authentication mode but does not in PAP or CHAP authentication mode.

Figure 1-10 802.1x re-authentication



802.1x re-authentication can be enabled in one of the following two ways:

- The RADIUS server has the switch perform 802.1x re-authentication of users. The RADIUS server sends the switch an Access-Accept packet with the Termination-Action attribute field of 1. Upon receiving the packet, the switch re-authenticates the user periodically.
- You enable 802.1x re-authentication on the switch. With 802.1x re-authentication enabled, the switch re-authenticates users periodically.

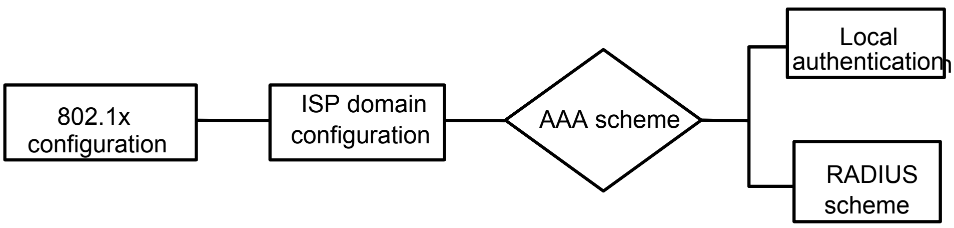
Note

802.1x re-authentication will fail if a CAMS server is used and configured to perform authentication but not accounting. This is because a CAMS server establishes a user session after it begins to perform accounting. Therefore, to enable 802.1x re-authentication, do not configure the **accounting none** command in the domain. This restriction does not apply to other types of servers.

Introduction to 802.1x Configuration

802.1x provides a solution for authenticating users. To implement this solution, you need to execute 802.1x-related commands. You also need to configure AAA schemes on switches and specify the authentication scheme (RADIUS or local authentication scheme).

Figure 1-11 802.1x configuration



- 802.1x users use domain names to associate with the ISP domains configured on switches
- Configure the AAA scheme (a local authentication scheme or a RADIUS scheme) to be adopted in the ISP domain.
- If you specify to use a local authentication scheme, you need to configure the user names and passwords manually on the switch. Users can pass the authentication through 802.1x client if they provide user names and passwords that match those configured on the switch.
- If you specify to adopt the RADIUS scheme, the supplicant systems are authenticated by a remote RADIUS server. In this case, you need to configure user names and passwords on the RADIUS server and perform RADIUS client-related configuration on the switches.
- You can also specify to adopt the RADIUS authentication scheme, with a local authentication scheme as a backup. In this case, the local authentication scheme is adopted when the RADIUS server fails.

Refer to the *AAA Operation* for detailed information about AAA scheme configuration.

Basic 802.1x Configuration

Configuration Prerequisites

- Configure ISP domain and the AAA scheme to be adopted. You can specify a RADIUS scheme or a local scheme.
- Ensure that the service type is configured as **lan-access** (by using the **service-type** command) if local authentication scheme is adopted.

Configuring Basic 802.1x Functions

Follow these steps to configure basic 802.1x functions:

To do…		Use the command…	Remarks
Enter system view		**system-view**	—
Enable 802.1x globally		**dot1x**	Required By default, 802.1x is disabled globally.
Enable 802.1x for specified ports	In system view	**dot1x interface** *interface-list*	Required By default, 802.1x is disabled on all ports.
	In port view	**interface** *interface-type interface-number*	
		dot1x	
		quit	
Set port authorization mode for specified ports	In system view	**dot1x port-control** { **authorized-force** | **unauthorized-force** | **auto** } [**interface** *interface-list*]	Optional By default, an 802.1x-enabled port operates in the **auto** mode.
	In port view	**interface** *interface-type interface-number*	
		dot1x port-control { **authorized-force** | **unauthorized-force** | **auto** }	
		quit	
Set access control method for specified ports	In system view	**dot1x port-method** { **macbased** | **portbased** } [**interface** *interface-list*]	Optional The default access control method on a port is MAC-based (that is, the **macbased** keyword is used by default).
	In port view	**interface** *interface-type interface-number*	
		dot1x port-method { **macbased** | **portbased** }	
		quit	
Set authentication method for 802.1x users		**dot1x authentication-method** { **chap** | **pap** | **eap** }	Optional By default, a switch performs CHAP authentication in EAP terminating mode.

To do…	Use the command…	Remarks
Enable online user handshaking	**dot1x handshake enable**	Optional By default, online user handshaking is enabled.

Caution

- 802.1x configurations take effect only after you enable 802.1x both globally and for specified ports.
- The settings of 802.1x and MAC address learning limit are mutually exclusive. Enabling 802.1x on a port will prevent you from setting the limit on MAC address learning on the port and vice versa.
- The settings of 802.1x and aggregation group member are mutually exclusive. Enabling 802.1x on a port will prevent you from adding the port to an aggregation group and vice versa.
- When the switch itself operates as an authentication server, its authentication method for 802.1x users cannot be configured as EAP.
- Handshake packets are used to test whether a user is online or not. Users need to run the proprietary client software of H3C to respond to the handshake packets.
- As clients not running the H3C client software do not support the online user handshaking function, switches cannot receive handshake acknowledgement packets from them in handshaking periods. To prevent users being falsely considered offline, you need to disable the online user handshaking function in this case.

Timer and Maximum User Number Configuration

Follow these steps to configure 802.1x timers and the maximum number of users:

To do…		Use the command...	Remarks
Enter system view		**system-view**	—
Set the maximum number of concurrent on-line users for specified ports	In system view	**dot1x max-user** *user-number* [**interface** *interface-list*]	Optional By default, a port can accommodate up to 256 users at a time.
	In port view	**interface** *interface-type interface-number*	
		dot1x max-user *user-number*	
		quit	
Set the maximum retry times to send request packets		**dot1x retry** *max-retry-value*	Optional By default, the maximum retry times to send a request packet is 2. That is, the authenticator system sends a request packet to a supplicant system for up to two times by default.

To do…	Use the command...	Remarks
Set 802.1x timers	**dot1x timer** { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* | **ver-period** *ver-period-value* }	Optional The settings of 802.1x timers are as follows. 1) handshake-period-value: 15 seconds 2) quiet-period-value: 60 seconds 3) server-timeout-value: 100 seconds 4) supp-timeout-value: 30 seconds 5) tx-period-value: 30 seconds 6) ver-period-value: 30 seconds
Enable the quiet-period timer	**dot1x quiet-period**	Optional By default, the quiet-period timer is disabled.

Note

- As for the **dot1x max-user** command, if you execute it in system view without specifying the *interface-list* argument, the command applies to all ports. You can also use this command in port view. In this case, this command applies to the current port only and the *interface-list* argument is not needed.
- As for the configuration of 802.1x timers, the default values are recommended.

Advanced 802.1x Configuration

Advanced 802.1x configurations, as listed below, are all optional.

- Configuration concerning CAMS, including multiple network adapters detecting, proxy detecting, and so on.
- Client version checking configuration
- DHCP–triggered authentication
- Guest VLAN configuration
- 802.1x re-authentication configuration
- Configuration of the 802.1x re-authentication timer

You need to configure basic 802.1x functions before configuring the above 802.1x features.

Configuring Proxy Checking

Follow these steps to configure proxy checking:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—

To do...		Use the command...	Remarks
Enable proxy checking function globally		**dot1x supp-proxy-check** { **logoff** | **trap** }	Required By default, the 802.1x proxy checking function is globally disabled.
Enable proxy checking for a port/specified ports	In system view	**dot1x supp-proxy-check** { **logoff** | **trap** } [**interface** *interface-list*]	Required By default, the 802.1x proxy checking is disabled on a port.
	In port view	**interface** *interface-type interface-number*	
		dot1x supp-proxy-check { **logoff** | **trap** }	
		quit	

Note

- The proxy checking function needs the cooperation of H3C's 802.1x client (iNode) program.
- The proxy checking function depends on the online user handshaking function. To enable the proxy detecting function, you need to enable the online user handshaking function first.
- The configuration listed in the above table takes effect only when it is performed on CAMS as well as on the switch. In addition, the client version checking function needs to be enabled on the switch too (by using the **dot1x version-check** command).

Configuring Client Version Checking

Follow these steps to configure client version checking:

To do...		Use the command...	Remarks
Enter system view		**system-view**	—
Enable 802.1x client version checking	In system view	**dot1x version-check** [**interface** *interface-list*]	Required By default, 802.1x client version checking is disabled on a port.
	In port view	**interface** *interface-type interface-number*	
		dot1x version-check	
		quit	
Set the maximum number of retires to send version checking request packets		**dot1x retry-version-max** *max-retry-version-value*	Optional By default, the maximum number of retires to send version checking request packets is 3.
Set the client version checking period timer		**dot1x timer ver-period** *ver-period-value*	Optional By default, the timer is set to 30 seconds.

Note

As for the **dot1x version-user** command, if you execute it in system view without specifying the *interface-list* argument, the command applies to all ports. You can also execute this command in port view. In this case, this command applies to the current port only and the *interface-list* argument is not needed.

Enabling DHCP-triggered Authentication

After performing the following configuration, 802.1x allows running DHCP on access users, and users are authenticated when they apply for dynamic IP addresses through DHCP.

Follow these steps to enable DHCP-triggered authentication:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable DHCP-triggered authentication	**dot1x dhcp-launch**	Required By default, DHCP-triggered authentication is disabled.

Configuring Guest VLAN

Follow these steps to configure guest VLAN:

<table>
<tr><th colspan="2">To do...</th><th>Use the command...</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="2">Configure the access control method of ports</td><td>dot1x port-method portbased</td><td>Required
The default access control method on a port is MAC-based. That is, the macbased keyword is used by default.</td></tr>
<tr><td rowspan="4">Enable the guest VLAN function</td><td>In system view</td><td>dot1x guest-vlan vlan-id [interface interface-list]</td><td rowspan="4">Required
By default, the guest VLAN function is disabled.</td></tr>
<tr><td rowspan="3">In port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>dot1x guest-vlan vlan-id</td></tr>
<tr><td>quit</td></tr>
</table>

Caution

- The guest VLAN function is available only when the switch operates in the port-based access control mode.
- Only one guest VLAN can be configured for each switch.
- The guest VLAN function cannot be implemented if you configure the **dot1x dhcp-launch** command on the switch to enable DHCP-triggered authentication. This is because the switch does not send authentication packets in that case.

Configuring 802.1x Re-Authentication

Follow these steps to enable 802.1x re-authentication:

To do...		Use the command...	Remarks
Enter system view		**system-view**	—
Enable 802.1x re-authentication on port(s)	In system view	**dot1x re-authenticate** [**interface** *interface-list*]	Required By default, 802.1x re-authentication is disabled on a port.
	In port view	**dot1x re-authenticate**	

Note

- To enable 802.1x re-authentication on a port, you must first enable 802.1x globally and on the port.
- When re-authenticating a user, a switch goes through the complete authentication process. It transmits the username and password of the user to the server. The server may authenticate the username and password, or, however, use re-authentication for only accounting and user connection status checking and therefore does not authenticate the username and password any more.
- An authentication server running CAMS authenticates the username and password during re-authentication of a user in the EAP authentication mode but does not in PAP or CHAP authentication mode.

Configuring the 802.1x Re-Authentication Timer

After 802.1x re-authentication is enabled on the switch, the switch determines the re-authentication interval in one of the following two ways:

- The switch uses the value of the Session-timeout attribute field of the Access-Accept packet sent by the RADIUS server as the re-authentication interval.
- The switch uses the value configured with the **dot1x timer reauth-period** command as the re-authentication interval for access users.

Note the following:

During re-authentication, the switch always uses the latest re-authentication interval configured, no matter which of the above-mentioned two ways is used to determine the re-authentication interval. For example, if you configure a re-authentication interval on the switch and the switch receives an Access-Accept packet whose Termination-Action attribute field is 1, the switch will ultimately use the value of the Session-timeout attribute field as the re-authentication interval.

The following introduces how to configure the 802.1x re-authentication timer on the switch.

Follow these steps to configure the re-authentication interval:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure a re-authentication interval	**dot1x timer reauth-period** *reauth-period-value*	Optional By default, the re-authentication interval is 3,600 seconds.

Displaying and Maintaining 802.1x Configuration

To do...	Use the command...	Remarks
Display the configuration, session, and statistics information about 802.1x	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]	Available in any view
Clear 802.1x-related statistics information	**reset dot1x statistics** [**interface** *interface-list*]	Available in user view

Configuration Example

802.1x Configuration Example

Network requirements

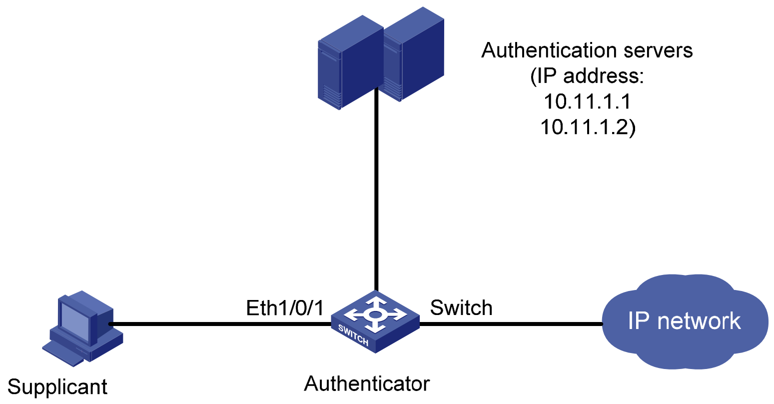
- Authenticate users on all ports to control their accesses to the Internet. The switch operates in MAC-based access control mode.
- All supplicant systems that pass the authentication belong to the default domain named "aabbcc.net". The domain can accommodate up to 30 users. As for authentication, a supplicant system is authenticated locally if the RADIUS server fails. And as for accounting, a supplicant system is disconnected by force if the RADIUS server fails. The name of an authenticated supplicant system is not suffixed with the domain name. A connection is terminated if the total size of the data passes through it during a period of 20 minutes is less than 2,000 bytes.
- The switch is connected to a server comprising of two RADIUS servers whose IP addresses are 10.11.1.1 and 10.11.1.2. The RADIUS server with an IP address of 10.11.1.1 operates as the primary authentication server and the secondary accounting server. The other operates as the secondary authentication server and primary accounting server. The password for the switch and the authentication RADIUS servers to exchange message is "name". And the password for the switch and the accounting RADIUS servers to exchange message is "money". The switch sends another packet to the RADIUS servers again if it sends a packet to the RADIUS server and does not receive response for 5 seconds, with the maximum number of retries of 5. And the switch sends

a real-time accounting packet to the RADIUS servers once in every 15 minutes. A user name is sent to the RADIUS servers with the domain name truncated.

- The user name and password for local 802.1x authentication are “localuser” and “localpass” (in plain text) respectively. The idle disconnecting function is enabled.

Network diagram

Figure 1-12 Network diagram for AAA configuration with 802.1x and RADIUS enabled



Configuration procedure

Note

Following configuration covers the major AAA/RADIUS configuration commands. Refer to *AAA Operation* for the information about these commands. Configuration on the client and the RADIUS servers is omitted.

Enable 802.1x globally.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] dot1x
```

Enable 802.1x on Ethernet 1/0/1.

```
[Sysname] dot1x interface Ethernet 1/0/1
```

Set the access control method to MAC-based (This operation can be omitted, as MAC-based is the default).

```
[Sysname] dot1x port-method macbased interface Ethernet 1/0/1
```

Create a RADIUS scheme named “radius1” and enter RADIUS scheme view.

```
[Sysname] radius scheme radius1
```

Assign IP addresses to the primary authentication and accounting RADIUS servers.

```
[Sysname-radius-radius1] primary authentication 10.11.1.1
[Sysname-radius-radius1] primary accounting 10.11.1.2
```

Assign IP addresses to the secondary authentication and accounting RADIUS server.

```
[Sysname-radius-radius1] secondary authentication 10.11.1.2
[Sysname-radius-radius1] secondary accounting 10.11.1.1
```

Set the password for the switch and the authentication RADIUS servers to exchange messages.

```
[Sysname-radius-radius1] key authentication name
```

Set the password for the switch and the accounting RADIUS servers to exchange messages.

```
[Sysname-radius-radius1] key accounting money
```

Set the interval and the number of the retries for the switch to send packets to the RADIUS servers.

```
[Sysname-radius-radius1] timer 5
[Sysname-radius-radius1] retry 5
```

Set the timer for the switch to send real-time accounting packets to the RADIUS servers.

```
[Sysname-radius-radius1] timer realtime-accounting 15
```

Configure to send the user name to the RADIUS server with the domain name truncated.

```
[Sysname-radius-radius1] user-name-format without-domain
[Sysname-radius-radius1] quit
```

Create the domain named “aabbcc.net” and enter its view.

```
[Sysname] domain aabbcc.net
```

Specify to adopt radius1 as the RADIUS scheme of the user domain. If RADIUS server is invalid, specify to adopt the local authentication scheme.

```
[Sysname-isp-aabbcc.net] scheme radius-scheme radius1 local
```

Specify the maximum number of users the user domain can accommodate to 30.

```
[Sysname-isp-aabbcc.net] access-limit enable 30
```

Enable the idle disconnecting function and set the related parameters.

```
[Sysname-isp-aabbcc.net] idle-cut enable 20 2000
[Sysname-isp-aabbcc.net] quit
```

Set the default user domain to **aabbcc.net**.

```
[Sysname] domain default enable aabbcc.net
```

Create a local access user account.

```
[Sysname] local-user localuser
[Sysname-luser-localuser] service-type lan-access
[Sysname-luser-localuser] password simple localpass
```

2 Quick EAD Deployment Configuration

When configuring quick EAD deployment, go to these sections for information you are interested in:

- Introduction to Quick EAD Deployment
- Configuring Quick EAD Deployment
- Displaying and Maintaining Quick EAD Deployment
- Quick EAD Deployment Configuration Example
- Troubleshooting

Introduction to Quick EAD Deployment

Quick EAD Deployment Overview

As an integrated solution, an Endpoint Admission Defense (EAD) solution can improve the overall defense power of a network. In real applications, however, deploying EAD clients proves to be time consuming and inconvenient.

To address the issue, the Switch 4500 provides the forcible deployment of EAD clients with 802.1x authentication, easing the work of EAD client deployment.

Operation of Quick EAD Deployment

Quick EAD deployment is achieved with the two functions: restricted access and HTTP redirection.

Restricted access

Before passing 802.1x authentication, a user is restricted (through ACLs) to a specific range of IP addresses or a specific server. Services like EAD client upgrading/download and dynamic address assignment are available on the specific server.

HTTP redirection

In the HTTP redirection approach, when the terminal users that have not passed 802.1x authentication access the Internet through Internet Explorer, they are redirected to a predefined URL for EAD client download.

The two functions ensure that all the users without an EAD client have downloaded and installed one from the specified server themselves before they can access the Internet, thus decreasing the complexity and effort that EAD client deployment may involve.

Note

The quick EAD deployment feature takes effect only when the authorization mode of an 802.1x-enabled port is set to **auto**.

Configuring Quick EAD Deployment

Configuration Prerequisites

- Enable 802.1x on the switch.
- Set the port authorization mode to **auto** for 802.1x-enabled ports using the **dot1x port-control** command.

Configuration Procedure

Configuring a free IP range

A free IP range is an IP range that users can access before passing 802.1x authentication.

Follow these steps to configure a free IP range:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure the URL for HTTP redirection	**dot1x url** *url-string*	Required
Configure a free IP range	**dot1x free-ip** *ip-address* { *mask-address* | *mask-length* }	Required By default, no free IP range is configured.

Caution

- You must configure the URL for HTTP redirection before configuring a free IP range. A URL must start with http:// and the segment where the URL resides must be in the free IP range. Otherwise, the redirection function cannot take effect.
- You must disable the DHCP-triggered authentication function of 802.1x before configuring a free IP range.
- With dot1x enabled but quick EAD deployment disabled, users cannot access the DHCP server if they fail 802.1x authentication. With quick EAD deployment enabled, users can obtain IP addresses dynamically before passing authentication if the IP address of the DHCP server is in the free IP range.
- The quick EAD deployment function applies to only ports with the authorization mode set to **auto** through the **dot1x port-control** command.
- At present, 802.1x is the only access approach that supports quick EAD deployment.
- Currently, the quick EAD deployment function does not support port security. The configured free IP range cannot take effect if you enable port security.
- The quick EAD deployment function and the MAC address authentication function are mutually exclusive. You cannot configure both the functions on the switch.

Setting the ACL timeout period

The quick EAD deployment function depends on ACLs in restricting access of users failing authentication. Each online user that has not passed authentication occupies a certain amount of ACL resources. After a user passes authentication, the occupied ACL resources will be released. When a

large number of users log in but cannot pass authentication, the switch may run out of ACL resources, preventing other users from logging in. A timer called ACL timer is designed to solve this problem.

You can control the usage of ACL resources by setting the ACL timer. The ACL timer starts once a user gets online. If the user has not passed authentication when the ACL timer expires, the occupied ACL resources are released for other users to use. When a tremendous of access requests are present, you can decrease the timeout period of the ACL timer appropriately for higher utilization of ACL resources.

Follow these steps to configure the ACL timer:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Set the ACL timer	**dot1x timer acl-timeout** *acl-timeout-value*	Required By default, the ACL timeout period is 30 minutes.

Displaying and Maintaining Quick EAD Deployment

To do...	Use the command...	Remarks
Display configuration information about quick EAD deployment	**display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]	Available in any view

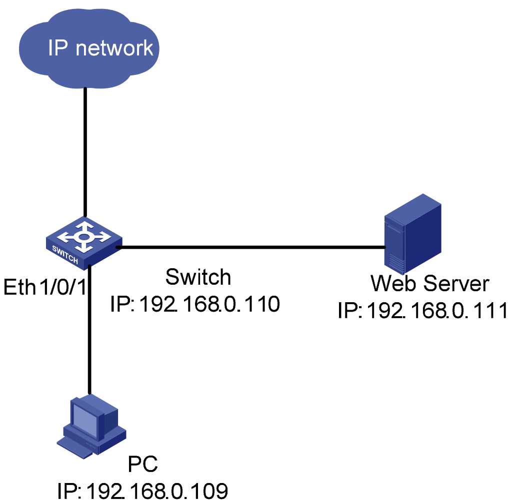
Quick EAD Deployment Configuration Example

Network requirements

A user connects to the switch directly. The switch connects to the Web server and the Internet. The user will be redirected to the Web server to download the authentication client and upgrade software when accessing the Internet through IE before passing authentication. After passing authentication, the user can access the Internet.

Network diagram

Figure 2-1 Network diagram for quick EAD deployment



Configuration procedure

Note

Before enabling quick EAD deployment, make sure sure that:

- The Web server is configured properly.
- The default gateway of the PC is configured as the IP address of the Layer-3 virtual interface of the VLAN to which the port that is directly connected with the PC belongs.

Configure the URL for HTTP redirection.

```
<Sysname> system-view
[Sysname] dot1x url http://192.168.0.111
```

Configure a free IP range.

```
[Sysname] dot1x free-ip 192.168.0.111 24
```

Set the ACL timer to 10 minutes.

```
[Sysname] dot1x timer acl-timeout 10
```

Enable dot1x globally.

```
[Sysname] dot1x
```

Enable dot1x for Ethernet 1/0/1.

```
[Sysname] dot1x interface Ethernet 1/0/1
```

Troubleshooting

Symptom: A user cannot be redirected to the specified URL server, no matter what URL the user enters in the IE address bar.

Solution:

- If a user enters an IP address in a format other than the dotted decimal notation, the user may not be redirected. This is related with the operating system used on the PC. In this case, the PC considers the IP address string a name and tries to resolve the name. If the resolution fails, the PC will access a specific website. Generally, this address is not in dotted decimal notation. As a result, the PC cannot receive any ARP response and therefore cannot be redirected. To solve this problem, the user needs to enter an IP address that is not in the free IP range in dotted decimal notation.
- If a user enters an address in the free IP range, the user cannot be redirected. This is because the switch considers that the user wants to access a host in the free IP range, unconcerned about whether this PC exists or not. To solve this problem, the user needs to enter an address not in the free IP range.
- Check that you have configured an IP address in the free IP range for the Web server and a correct URL for redirection, and that the server provides Web services properly.

3 HABP Configuration

When configuring HABP, go to these sections for information you are interested in:

- Introduction to HABP
- HABP Server Configuration
- HABP Client Configuration
- Displaying and Maintaining HABP Configuration

Introduction to HABP

When a switch is configured with the 802.1x function, 802.1x will authenticate and authorize 802.1x-enabled ports and allow only the authorized ports to forward packets. In case a port fails 802.1x authentication and authorization, service packets from and to that port will be blocked, making it impossible to manage the switch attached to the port. The Huawei Authentication Bypass Protocol (HABP) aims at solving this problem.

An HABP packet carries the MAC addresses of the attached switches with it. It can bypass the 802.1x authentications when traveling between HABP-enabled switches, through which management devices can obtain the MAC addresses of the attached switches and thus the management of the attached switches is feasible.

HABP is built on the client-server model. Typically, the HABP server sends HABP requests to the client periodically to collect the MAC address(es) of the attached switch(es). The client responds to the requests, and forwards the HABP requests to the attached switch(es). The HABP server usually runs on the administrative device while the HABP client runs on the attached switches.

For ease of switch management, it is recommended that you enable HABP for 802.1x-enabled switches.

HABP Server Configuration

With the HABP server launched, a management device sends HABP request packets regularly to the attached switches to collect their MAC addresses. You need also to configure the interval on the management device for an HABP server to send HABP request packets.

Follow these steps to configure an HABP server:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable HABP	**habp enable**	Optional By default, HABP is enabled.

To do...	Use the command...	Remarks
Configure the current switch to be an HABP server	**habp server vlan** *vlan-id*	Required By default, a switch operates as an HABP client after you enable HABP on the switch. If you want to use the switch as a management switch, you need to configure the switch to be an HABP server.
Configure the interval to send HABP request packets.	**habp timer** *interval*	Optional The default interval for an HABP server to send HABP request packets is 20 seconds.

HABP Client Configuration

HABP clients reside on switches attached to HABP servers. After you enable HABP for a switch, the switch operates as an HABP client by default. So you only need to enable HABP on a switch to make it an HABP client.

Follow these steps to configure an HABP client:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable HABP	**habp enable**	Optional HABP is enabled by default. And a switch operates as an HABP client after you enable HABP for it.

Displaying and Maintaining HABP Configuration

To do...	Use the command...	Remarks
Display HABP configuration and status	**display habp**	Available in any view
Display the MAC address table maintained by HABP	**display habp table**	Available in any view
Display statistics on HABP packets	**display habp traffic**	Available in any view

4 System Guard Configuration

When configuring System Guard, go to these sections for information you are interested in:

- System Guard Overview
- Configuring System Guard
- Displaying and Maintaining System Guard Configuration

System Guard Overview

Guard Against IP Attacks

System-guard operates to inspect the IP packets over 10-second intervals for the CPU for suspicious source IP addresses. Once the packets from such an IP address hit the predefined threshold, the switch with System Guard enabled will take the following action: If the packets from the source IP address need to be processed by the CPU, the switch decreases the precedence of delivering such packets to the CPU.

Guard Against TCN Attacks

System Guard monitors the rate at which TCN/TC packets are received on the ports. If a port receives an excessive number of TCN/TC packets within a given period of time, the switch sends only one TCN/TC packet in every 10 seconds to the CPU and discards the rest TCN/TC packets, while outputting trap and log information.

Layer 3 Error Control

With the Layer 3 error control feature enabled, the switch delivers all Layer 3 packets that the switch considers to be error packets to the CPU.

Configuring System Guard

Configuring System Guard Against IP Attacks

Configuration of System Guard against IP attacks includes these tasks:

- Enabling System Guard against IP attacks
- Setting the maximum number of infected hosts that can be concurrently monitored
- Configuring parameters related to MAC address learning

Follow these steps to configure System Guard against IP attacks:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable System Guard against IP attacks	**system-guard ip enable**	Required Disabled by default

To do...	Use the command...	Remarks
Set the maximum number of infected hosts that can be concurrently monitored	**system-guard ip detect-maxnum** *number*	Optional 30 by default
Set the maximum number of addresses that the system can learn, the maximum number of times an address can be hit before an action is taken and the address isolation time (presented in the number of multiples of MAC address aging time)	**system-guard ip detect-threshold** *ip-record-threshold record-times-threshold isolate-time*	Optional By default, *ip-record-threshold* is 30; *record-times-threshold* is 1, and *isolate-time* is 3.

Note

The correlations among the arguments of the **system-guard ip detect-threshold** command can be clearly described with this example: If you set *ip-record-threshold*, *record-times-threshold* and *isolate-time* to 30, 1 and 3 respectively, when the system detects successively three times that over 50 IP packets (destined for an address other that an IP address of the switch) from a source IP address are received within a period of 10 seconds, the system considers that it is being attacked —the system sorts out the source IP address and decreases the precedence of delivering packets from the source IP address to the CPU for a period of 5 times the MAC address aging time.

Configuring System Guard Against TCN Attacks

Configuration of System Guard against TCN attacks includes these tasks:

- Enabling System Guard against TCN attacks
- Setting the threshold of TCN/TC packet receiving rate

Follow these steps to configure System Guard against TCN attacks:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable System Guard against TCN attacks	**system-guard tcn enable**	Required Disabled by default
Set the threshold of TCN/TC packet receiving rate	**system-guard tcn rate-threshold** *rate-threshold*	Optional 1 pps by default

Note

As the system monitoring cycle is 10 seconds, the system sends trap and log information if more than 10 TCN/TC packets are received within 10 seconds by default. If the TCN/TC packet receiving rate is lower than the set threshold within a 10-second monitoring cycle, the system will not send trap or log information in the next 10-second monitoring cycle.

Enabling Layer 3 Error Control

Follow these steps to enable Layer 3 error control:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable Layer 3 error control	**system-guard l3err enable**	Required Enabled by default

Displaying and Maintaining System Guard Configuration

To do...	Use the command...	Remarks
Display the monitoring result and parameter settings of System Guard against IP attacks	**display system-guard ip state**	Available in any view
Display the information about IP packets received by the CPU	**display system-guard ip-record**	
Display the status of Layer 3 error control	**display system-guard l3err state**	
Display the status of TCN	**display system-guard tcn state**	

Table of Contents

1 AAA Overview

Introduction to AAA

AAA is the acronym for the three security functions: authentication, authorization and accounting. It provides a uniform framework for you to configure these three functions to implement network security management.

- Authentication: Defines what users can access the network,
- Authorization: Defines what services can be available to the users who can access the network, and
- Accounting: Defines how to charge the users who are using network resources.

Typically, AAA operates in the client/server model: the client runs on the managed resources side while the server stores the user information. Thus, AAA is well scalable and can easily implement centralized management of user information.

Authentication

AAA supports the following authentication methods:

- None authentication: Users are trusted and are not checked for their validity. Generally, this method is not recommended.
- Local authentication: User information (including username, password, and some other attributes) is configured on this device, and users are authenticated on this device instead of on a remote device. Local authentication is fast and requires lower operational cost, but has the deficiency that information storage capacity is limited by device hardware.
- Remote authentication: Users are authenticated remotely through RADIUS protocol. This device (for example, a 3Com switch) acts as the client to communicate with the RADIUS or TACACS server. Remote authentication allows convenient centralized management and is feature-rich. However, to implement remote authentication, a server is needed and must be configured properly.

Authorization

AAA supports the following authorization methods:

- Direct authorization: Users are trusted and directly authorized.
- Local authorization: Users are authorized according to the related attributes configured for their local accounts on this device.
- RADIUS authorization: Users are authorized after they pass RADIUS authentication. In RADIUS protocol, authentication and authorization are combined together, and authorization cannot be performed alone without authentication.

Accounting

AAA supports the following accounting methods:

- None accounting: No accounting is performed for users.
- Remote accounting: User accounting is performed on a remote RADIUS or TACACS server.

Introduction to ISP Domain

An Internet service provider (ISP) domain is a group of users who belong to the same ISP. For a username in the format of userid@isp-name or userid.isp-name, the isp-name following the "@" character is the ISP domain name. The access device uses userid as the username for authentication, and isp-name as the domain name.

In a multi-ISP environment, the users connected to the same access device may belong to different domains. Since the users of different ISPs may have different attributes (such as different forms of username and password, different service types/access rights), it is necessary to distinguish the users by setting ISP domains.

You can configure a set of ISP domain attributes (including AAA policy, RADIUS scheme, and so on) for each ISP domain independently in ISP domain view.

Introduction to AAA Services

Introduction to RADIUS

AAA is a management framework. It can be implemented by not only one protocol. But in practice, the most commonly used service for AAA is RADIUS.

What is RADIUS

Remote Authentication Dial-in User Service (RADIUS) is a distributed service based on client/server structure. It can prevent unauthorized access to your network and is commonly used in network environments where both high security and remote user access service are required.

The RADIUS service involves three components:

- Protocol: Based on the UDP/IP layer, RFC 2865 and 2866 define the message format and message transfer mechanism of RADIUS, and define 1812 as the authentication port and 1813 as the accounting port.
- Server: RADIUS Server runs on a computer or workstation at the center. It stores and maintains user authentication information and network service access information.
- Client: RADIUS Client runs on network access servers throughout the network.

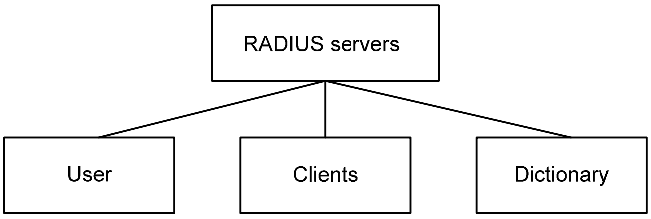
RADIUS operates in the client/server model.

- A switch acting as a RADIUS client passes user information to a specified RADIUS server, and takes appropriate action (such as establishing/terminating user connection) depending on the responses returned from the server.
- The RADIUS server receives user connection requests, authenticates users, and returns all required information to the switch.

Generally, a RADIUS server maintains the following three databases (see Figure 1-1):

- Users: This database stores information about users (such as username, password, protocol adopted and IP address).
- Clients: This database stores information about RADIUS clients (such as shared key).
- Dictionary: The information stored in this database is used to interpret the attributes and attribute values in the RADIUS protocol.

Figure 1-1 Databases in a RADIUS server

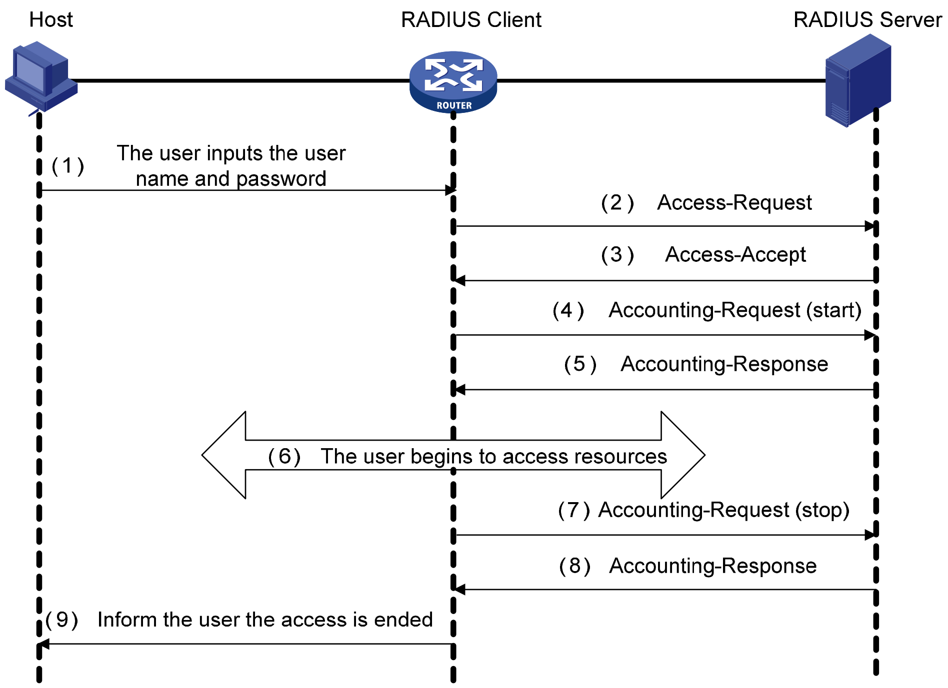


In addition, a RADIUS server can act as a client of some other AAA server to provide authentication or accounting proxy service.

Basic message exchange procedure in RADIUS

The messages exchanged between a RADIUS client (a switch, for example) and a RADIUS server are verified through a shared key. This enhances the security. The RADIUS protocol combines the authentication and authorization processes together by sending authorization information along with the authentication response message. Figure 1-2 depicts the message exchange procedure between user, switch and RADIUS server.

Figure 1-2 Basic message exchange procedure of RADIUS



The basic message exchange procedure of RADIUS is as follows:

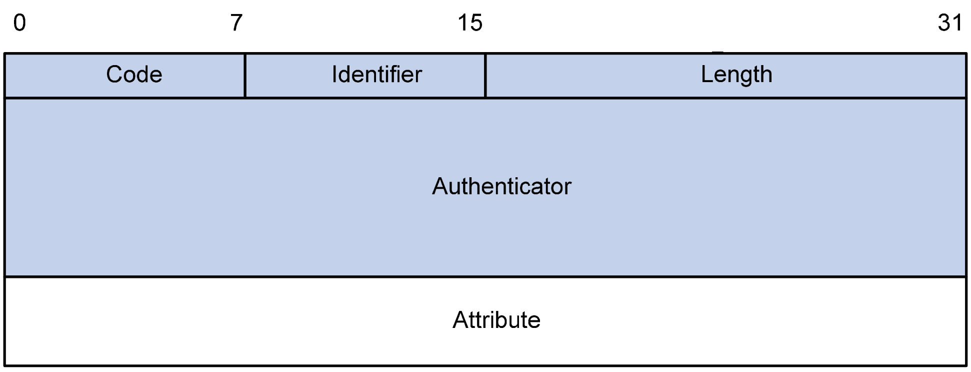
1) The user enters the username and password.
2) The RADIUS client receives the username and password, and then sends an authentication request (Access-Request) to the RADIUS server.
3) The RADIUS server compares the received user information with that in the Users database to authenticate the user. If the authentication succeeds, the RADIUS server sends back to the RADIUS client an authentication response (Access-Accept), which contains the user's authorization information. If the authentication fails, the server returns an Access-Reject response.

4) The RADIUS client accepts or denies the user depending on the received authentication result. If it accepts the user, the RADIUS client sends a start-accounting request (Accounting-Request, with the Status-Type attribute value = start) to the RADIUS server.
5) The RADIUS server returns a start-accounting response (Accounting-Response).
6) The user starts to access network resources.
7) The RADIUS client sends a stop-accounting request (Accounting-Request, with the Status-Type attribute value = stop) to the RADIUS server.
8) The RADIUS server returns a stop-accounting response (Accounting-Response).
9) The access to network resources is ended.

RADIUS message format

RADIUS messages are transported over UDP, which does not guarantee reliable delivery of messages between RADIUS server and client. As a remedy, RADIUS adopts the following mechanisms: timer management, retransmission, and backup server. Figure 1-3 depicts the format of RADIUS messages.

Figure 1-3 RADIUS message format



1) The Code field (one byte) decides the type of RADIUS message, as shown in Table 1-1.

Table 1-1 Description on the major values of the Code field

Code	Message type	Message description
1	Access-Request	Direction: client->server. The client transmits this message to the server to determine if the user can access the network. This message carries user information. It must contain the User-Name attribute and may contain the following attributes: NAS-IP-Address, User-Password and NAS-Port.
2	Access-Accept	Direction: server->client. The server transmits this message to the client if all the attribute values carried in the Access-Request message are acceptable (that is, the user passes the authentication).
3	Access-Reject	Direction: server->client. The server transmits this message to the client if any attribute value carried in the Access-Request message is unacceptable (that is, the user fails the authentication).

Code	Message type	Message description
4	Accounting-Request	Direction: client->server. The client transmits this message to the server to request the server to start or end the accounting (whether to start or to end the accounting is determined by the Acct-Status-Type attribute in the message). This message carries almost the same attributes as those carried in the Access-Request message.
5	Accounting-Response	Direction: server->client. The server transmits this message to the client to notify the client that it has received the Accounting-Request message and has correctly recorded the accounting information.

2) The Identifier field (one byte) is used to match requests and responses. It changes whenever the content of the Attributes field changes, and whenever a valid response has been received for a previous request, but remains unchanged for message retransmission.
3) The Length field (two bytes) specifies the total length of the message (including the Code, Identifier, Length, Authenticator and Attributes fields). The bytes beyond the length are regarded as padding and are ignored upon reception. If a received message is shorter than what the Length field indicates, it is discarded.
4) The Authenticator field (16 bytes) is used to authenticate the response from the RADIUS server; and is used in the password hiding algorithm. There are two kinds of authenticators: Request Authenticator and Response Authenticator.
5) The Attributes field contains specific authentication/authorization/accounting information to provide the configuration details of a request or response message. This field contains a list of field triplet (Type, Length and Value):

- The Type field (one byte) specifies the type of an attribute. Its value ranges from 1 to 255. Table 1-2 lists the attributes that are commonly used in RADIUS authentication/authorization.
- The Length field (one byte) specifies the total length of the attribute in bytes (including the Type, Length and Value fields).
- The Value field (up to 253 bytes) contains the information of the attribute. Its format is determined by the Type and Length fields.

Table 1-2 RADIUS attributes

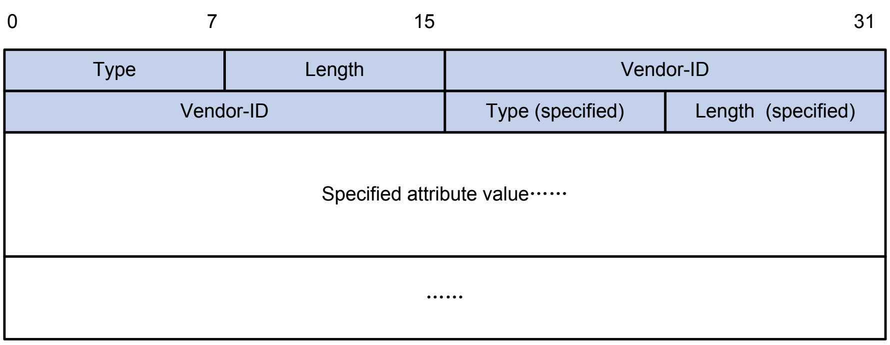
Type field value	Attribute type	Type field value	Attribute type
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id

Type field value	Attribute type	Type field value	Attribute type
10	Framed-Routing	32	NAS-Identifier
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply-Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-ID	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

The RADIUS protocol has good scalability. Attribute 26 (Vender-Specific) defined in this protocol allows a device vendor to extend RADIUS to implement functions that are not defined in standard RADIUS.

Figure 1-4 depicts the format of attribute 26. The Vendor-ID field used to identify a vendor occupies four bytes, where the first byte is 0, and the other three bytes are defined in RFC 1700. Here, the vendor can encapsulate multiple customized sub-attributes (containing vendor-specific Type, Length and Value) to implement a RADIUS extension.

Figure 1-4 Vendor-specific attribute format



2 AAA Configuration

AAA Configuration Task List

You need to configure AAA to provide network access services for legal users while protecting network devices and preventing unauthorized access and repudiation behavior.

Complete the following tasks to configure AAA (configuring a combined AAA scheme for an ISP domain):

<table>
<tr><th colspan="3">Task</th><th>Remarks</th></tr>
<tr><td rowspan="8">AAA configuration</td><td colspan="2">Creating an ISP Domain and Configuring Its Attributes</td><td>Required</td></tr>
<tr><td colspan="2">Configuring a combined AAA scheme</td><td>Required</td></tr>
<tr><td rowspan="3">Configuring an AAA Scheme for an ISP Domain</td><td>None authentication</td><td rowspan="3">• Use one of the authentication methods
• You need to configure RADIUS before performing RADIUS authentication</td></tr>
<tr><td>Local authentication</td></tr>
<tr><td>RADIUS authentication</td></tr>
<tr><td colspan="2">Configuring Dynamic VLAN Assignment</td><td>Optional</td></tr>
<tr><td colspan="2">Configuring the Attributes of a Local User</td><td>Optional</td></tr>
<tr><td colspan="2">Cutting Down User Connections Forcibly</td><td>Optional</td></tr>
</table>

Complete the following tasks to configure AAA (configuring separate AAA schemes for an ISP domain):

Task		Remarks
AAA configuration	Creating an ISP Domain and Configuring Its Attributes	Required
	Configuring separate AAA schemes	Required
	Configuring an AAA Scheme for an ISP Domain	Required With separate AAA schemes, you can specify authentication, authorization and accounting schemes respectively. You need to configure RADIUS or HWATACACS before performing RADIUS authentication.
	Configuring Dynamic VLAN Assignment	Optional
	Configuring the Attributes of a Local User	Optional
	Cutting Down User Connections Forcibly	Optional

Creating an ISP Domain and Configuring Its Attributes

Follow these steps to create an ISP domain and configure its attributes:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an ISP domain or set an ISP domain as the default ISP domain	**domain** { *isp-name* | **default** { **disable** | **enable** *isp-name* } }	Required If no ISP domain is set as the default ISP domain, the ISP domain "system" is used as the default ISP domain.
Set the status of the ISP domain	**state** { **active** | **block** }	Optional By default, an ISP domain is in the **active** state, that is, all the users in the domain are allowed to request network service.
Set the maximum number of access users that the ISP domain can accommodate	**access-limit** { **disable** | **enable** *max-user-number* }	Optional By default, there is no limit on the number of access users that the ISP domain can accommodate.
Set the idle-cut function	**idle-cut** { **disable** | **enable** *minute flow* }	Optional By default, the idle-cut function is disabled.
Set the accounting-optional switch	**accounting optional**	Optional By default, the accounting-optional switch is off.

To do…	Use the command…	Remarks
Set the messenger function	**messenger time** { **enable** *limit interval* | **disable** }	Optional By default, the messenger function is disabled.
Set the self-service server location function	**self-service-url** { **disable** | **enable** *url-string* }	Optional By default, the self-service server location function is disabled.

Note that:

- On a Switch 4500, each access user belongs to an ISP domain. You can configure up to 16 ISP domains on the switch. When a user logs in, if no ISP domain name is carried in the username, the switch assumes that the user belongs to the default ISP domain.
- As the delimiter, the "@" must not appear more than once in the username.
- If the system does not find any available accounting server or fails to communicate with any accounting server when it performs accounting for a user, it does not disconnect the user as long as the accounting optional command has been executed, though it cannot perform accounting for the user in this case.
- The self-service server location function needs the cooperation of a RADIUS server that supports self-service, such as Comprehensive Access Management Server (CAMS). Through self-service, users can manage and control their account or card numbers by themselves. A server installed with self-service software is called a self-service server.

Note

H3C's CAMS Server is a service management system used to manage networks and ensure network and user information security. With the cooperation of other networking devices (such as switches) in a network, a CAMS server can implement the AAA functions and right management.

Configuring an AAA Scheme for an ISP Domain

You can configure either a combined AAA scheme or separate AAA schemes.

Configuring a combined AAA scheme

You can use the **scheme** command to specify an AAA scheme for an ISP domain.

Follow these steps to configure a combined AAA scheme:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	**domain** *isp-name*	Required

To do…	Use the command…	Remarks
Configure an AAA scheme for the ISP domain	**scheme** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }	Required By default, an ISP domain uses the **local** AAA scheme.

Caution

- You can execute the **scheme radius-scheme** *radius-scheme-name* command to adopt an already configured RADIUS scheme to implement all the three AAA functions. If you adopt the local scheme, only the authentication and authorization functions are implemented, the accounting function cannot be implemented.
- If you execute the **scheme radius-scheme** *radius-scheme-name* **local** command, the local scheme is used as the secondary scheme in case no RADIUS server is available. That is, if the communication between the switch and a RADIUS server is normal, the local scheme is not used; otherwise, the local scheme is used.
- If you execute the **scheme local** or **scheme none** command to adopt **local** or **none** as the primary scheme, the local authentication is performed or no authentication is performed. In this case you cannot specify any RADIUS scheme at the same time.
- If you configure to use **none** as the primary scheme, FTP users of the domain cannot pass authentication. Therefore, you cannot specify **none** as the primary scheme if you want to enable FTP service.

Configuring separate AAA schemes

You can use the **authentication**, **authorization**, and **accounting** commands to specify a scheme for each of the three AAA functions (authentication, authorization and accounting) respectively. The following gives the implementations of this separate way for the services supported by AAA.

1) For terminal users

- Authentication: RADIUS, local or none.
- Authorization: none.
- Accounting: RADIUS or none.

You can use an arbitrary combination of the above implementations for your AAA scheme configuration.

2) For FTP users

Only authentication is supported for FTP users.

Authentication: RADIUS, local.

Follow these steps to configure separate AAA schemes:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an ISP domain and enter its view, or enter the view of an existing ISP domain	**domain** *isp-name*	Required

To do…	Use the command…	Remarks
Configure an authentication scheme for the ISP domain	**authentication** { **radius-scheme** *radius-scheme-name* [**local**] | **local** | **none** }	Optional By default, no separate authentication scheme is configured.
Configure an authorization scheme for the ISP domain	**authorization** { **none** }	Optional By default, no separate authorization scheme is configured.
Configure an accounting scheme for the ISP domain	**accounting** { **none** | **radius-scheme** *radius-scheme-name* }	Optional By default, no separate accounting scheme is configured.

Note

- If a combined AAA scheme is configured as well as the separate authentication, authorization and accounting schemes, the separate ones will be adopted in precedence.
- RADIUS scheme and local scheme do not support the separation of authentication and authorization. Therefore, pay attention when you make authentication and authorization configuration for a domain: When the **scheme radius-scheme** or **scheme local** command is executed and the **authentication** command is not executed, the authorization information returned from the RADIUS or local scheme still takes effect even if the **authorization none** command is executed.

Configuration guidelines

Suppose a combined AAA scheme is available. The system selects AAA schemes according to the following principles:

- If authentication, authorization, accounting each have a separate scheme, the separate schemes are used.
- If you configure only a separate authentication scheme (that is, there are no separate authorization and accounting schemes configured), the combined scheme is used for authorization and accounting. In this case, if the combined scheme uses RADIUS , the system never uses the secondary scheme for authorization and accounting.
- If you configure no separate scheme, the combined scheme is used for authentication, authorization, and accounting. In this case, if the system uses the secondary local scheme for authentication, it also does so for authorization and accounting; if the system uses the first scheme for authentication, it also does so for authorization and accounting, even if authorization and accounting fail.

Configuring Dynamic VLAN Assignment

The dynamic VLAN assignment feature enables a switch to dynamically add the switch ports of successfully authenticated users to different VLANs according to the attributes assigned by the RADIUS server, so as to control the network resources that different users can access.

Currently, the switch supports the following two types of assigned VLAN IDs: integer and string.

- Integer: If the RADIUS authentication server assigns integer type of VLAN IDs, you can set the VLAN assignment mode to integer on the switch (this is also the default mode on the switch). Then, upon receiving an integer ID assigned by the RADIUS authentication server, the switch adds the port to the VLAN whose VLAN ID is equal to the assigned integer ID. If no such a VLAN exists, the switch first creates a VLAN with the assigned ID, and then adds the port to the newly created VLAN.
- String: If the RADIUS authentication server assigns string type of VLAN IDs, you can set the VLAN assignment mode to string on the switch. Then, upon receiving a string ID assigned by the RADIUS authentication server, the switch compares the ID with existing VLAN names on the switch. If it finds a match, it adds the port to the corresponding VLAN. Otherwise, the VLAN assignment fails and the user fails the authentication.

In actual applications, to use this feature together with Guest VLAN, you should better set port control to port-based mode. For more information, refer to Basic 802.1x Configuration of *802.1x and System Guard Operation.*

Follow these steps to configure dynamic VLAN assignment:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create an ISP domain and enter its view	**domain** *isp-name*	—
Set the VLAN assignment mode	**vlan-assignment-mode** { **integer** | **string** }	Optional By default, the VLAN assignment mode is integer.
Create a VLAN and enter its view	**vlan** *vlan-id*	—
Set a VLAN name for VLAN assignment	**name** *string*	This operation is required if the VLAN assignment mode is set to string.

Caution

- In string mode, if the VLAN ID assigned by the RADIUS server is a character string containing only digits (for example, 1024), the switch first regards it as an integer VLAN ID: the switch transforms the string to an integer value and judges if the value is in the valid VLAN ID range; if it is, the switch adds the authenticated port to the VLAN with the integer value as the VLAN ID (VLAN 1024, for example).
- To implement dynamic VLAN assignment on a port where both MSTP and 802.1x are enabled, you must set the MSTP port to an edge port.

Configuring the Attributes of a Local User

When **local** scheme is chosen as the AAA scheme, you should create local users on the switch and configure the relevant attributes.

The local users are users set on the switch, with each user uniquely identified by a username. To make a user who is requesting network service pass local authentication, you should add an entry in the local user database on the switch for the user.

Follow these steps to configure the attributes of a local user:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the password display mode of all local users	**local-user password-display-mode** { **cipher-force** | **auto** }	Optional By default, the password display mode of all access users is **auto**, indicating the passwords of access users are displayed in the modes set by the **password** command.
Add a local user and enter local user view	**local-user** *user-name*	Required By default, there is no local user in the system.
Set a password for the local user	**password** { **simple** | **cipher** } *password*	Required
Set the status of the local user	**state** { **active** | **block** }	Optional By default, the user is in **active** state, that is, the user is allowed to request network services.
Authorize the user to access specified type(s) of service	**service-type** { **ftp** | **lan-access** | { **telnet** | **ssh** | **terminal** }* [**level** *level*] }	Required By default, the system does not authorize the user to access any service.
Set the privilege level of the user	**level** *level*	Optional By default, the privilege level of the user is 0.
Configure the authorized VLAN for the local user	**authorization vlan** *string*	Required By default, no authorized VLAN is configured for the local user.
Set the attributes of the user whose service type is lan-access	**attribute** { **ip** *ip-address* | **mac** *mac-address* | **idle-cut** *second* | **access-limit** *max-user-number* | **vlan** *vlan-id* | **location** { **nas-ip** *ip-address* **port** *port-number* | **port** *port-number* } }*	Optional When binding the user to a remote port, you must use **nas-ip** *ip-address* to specify a remote access server IP address (here, *ip-address* is 127.0.0.1 by default, representing this device). When binding the user to a local port, you need not use **nas-ip** *ip-address*.

Caution

- The following characters are not allowed in the *user-name* string: /:*?<>. And you cannot input more than one “@” in the string.
- After the **local-user password-display-mode cipher-force** command is executed, any password will be displayed in cipher mode even though you specify to display a user password in plain text by using the **password** command.
- If a username and password is required for user authentication (RADIUS authentication as well as local authentication), the command level that a user can access after login is determined by the privilege level of the user. For SSH users using RSA shared key for authentication, the commands they can access are determined by the levels set on their user interfaces.
- If the configured authentication method is none or password authentication, the command level that a user can access after login is determined by the level of the user interface.
- If the clients connected to a port have different authorized VLANs, only the first client passing the MAC address authentication can be assigned with an authorized VLAN. The switch will not assign authorized VLANs for subsequent users passing MAC address authentication. In this case, you are recommended to connect only one MAC address authentication user or multiple users with the same authorized VLAN to a port.
- For local **RADIUS** authentication to take effect, the VLAN assignment mode must be set to **string** after you specify authorized VLANs for local users.

Cutting Down User Connections Forcibly

Follow these steps to cut down user connections forcibly:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Cut down user connections forcibly	**cut connection** { **all** | **access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name* }	Required

Note

You can use the **display connection** command to view the connections of Telnet users, but you cannot use the **cut connection** command to cut down their connections.

RADIUS Configuration Task List

3Com’s Ethernet switches can function not only as RADIUS clients but also as local RADIUS servers.

Complete the following tasks to configure RADIUS (the switch functions as a RADIUS client):

Task		Remarks
Configuring the RADIUS client	Creating a RADIUS Scheme	Required
	Configuring RADIUS Authentication/Authorization Servers	Required
	Configuring RADIUS Accounting Servers	Required
	Configuring Shared Keys for RADIUS Messages	Optional
	Configuring the Maximum Number of RADIUS Request Transmission Attempts	Optional
	Configuring the Type of RADIUS Servers to be Supported	Optional
	Configuring the Status of RADIUS Servers	Optional
	Configuring the Attributes of Data to be Sent to RADIUS Servers	Optional
	Configuring Timers for RADIUS Servers	Optional
	Enabling Sending Trap Message when a RADIUS Server Goes Down	Optional
	Enabling the User Re-Authentication at Restart Function	Optional
Configuring the RADIUS server	Refer to the configuration of the RADIUS Server.	—

Complete the following tasks to configure RADIUS (the switch functions as a local RADIUS server):

Task		Remarks
Configuring the RADIUS server	Creating a RADIUS Scheme	Required
	Configuring RADIUS Authentication/Authorization Servers	Required
	Configuring RADIUS Accounting Servers	Required
	Configuring Shared Keys for RADIUS Messages	Optional
	Configuring the Maximum Number of RADIUS Request Transmission Attempts	Optional
	Configuring the Type of RADIUS Servers to be Supported	Optional
	Configuring the Status of RADIUS Servers	Optional
	Configuring the Attributes of Data to be Sent to RADIUS Servers	Optional
	Configuring the Local RADIUS Server	Required
	Configuring Timers for RADIUS Servers	Optional
	Enabling Sending Trap Message when a RADIUS Server Goes Down	Optional
Configuring the RADIUS client	Refer to the configuration of the RADIUS client	—

The RADIUS service configuration is performed on a RADIUS scheme basis. In an actual network environment, you can either use a single RADIUS server or two RADIUS servers (primary and secondary servers with the same configuration but different IP addresses) in a RADIUS scheme. After

creating a new RADIUS scheme, you should configure the IP address and UDP port number of each RADIUS server you want to use in this scheme. These RADIUS servers fall into two types: authentication/authorization, and accounting. And for each type of server, you can configure two servers in a RADIUS scheme: primary server and secondary server. A RADIUS scheme has some parameters such as IP addresses of the primary and secondary servers, shared keys, and types of the RADIUS servers.

In an actual network environment, you can configure the above parameters as required. But you should configure at least one authentication/authorization server and one accounting server, and you should keep the RADIUS server port settings on the switch consistent with those on the RADIUS servers.

Note

Actually, the RADIUS service configuration only defines the parameters for information exchange between switch and RADIUS server. To make these parameters take effect, you must reference the RADIUS scheme configured with these parameters in an ISP domain view (refer to AAA Configuration).

Creating a RADIUS Scheme

The RADIUS protocol configuration is performed on a RADIUS scheme basis. You should first create a RADIUS scheme and enter its view before performing other RADIUS protocol configurations.

Follow these steps to create a RADIUS scheme:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable RADIUS authentication port	**radius client enable**	Optional By default, RADIUS authentication port is enabled.
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.

Note

A RADIUS scheme can be referenced by multiple ISP domains simultaneously.

Configuring RADIUS Authentication/Authorization Servers

Follow these steps to configure RADIUS authentication/authorization servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the IP address and port number of the primary RADIUS authentication/authorization server	**primary authentication** *ip-address* [*port-number*]	Required By default, the IP address and UDP port number of the primary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.
Set the IP address and port number of the secondary RADIUS authentication/authorization server	**secondary authentication** *ip-address* [*port-number*]	Optional By default, the IP address and UDP port number of the secondary server are 0.0.0.0 and 1812 respectively for a newly created RADIUS scheme.

Note

- The authentication response sent from the RADIUS server to the RADIUS client carries authorization information. Therefore, you need not (and cannot) specify a separate RADIUS authorization server.
- In an actual network environment, you can specify one server as both the primary and secondary authentication/authorization servers, as well as specifying two RADIUS servers as the primary and secondary authentication/authorization servers respectively.
- The IP address and port number of the primary authentication server used by the default RADIUS scheme "system" are 127.0.0.1 and 1645.

Configuring RADIUS Accounting Servers

Follow these steps to configure RADIUS accounting servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the IP address and port number of the primary RADIUS accounting server	**primary accounting** *ip-address* [*port-number*]	Required By default, the IP address and UDP port number of the primary accounting server are 0.0.0.0 and 1813 for a newly created RADIUS scheme.

To do…	Use the command…	Remarks
Set the IP address and port number of the secondary RADIUS accounting server	**secondary accounting** *ip-address* [*port-number*]	Optional By default, the IP address and UDP port number of the secondary accounting server are 0.0.0.0 and 1813 for a newly created RADIUS scheme.
Enable stop-accounting request buffering	**stop-accounting-buffer enable**	Optional By default, stop-accounting request buffering is enabled.
Set the maximum number of transmission attempts of a buffered stop-accounting request.	**retry stop-accounting** *retry-times*	Optional By default, the system tries at most 500 times to transmit a buffered stop-accounting request.
Set the maximum allowed number of continuous real-time accounting failures	**retry realtime-accounting** *retry-times*	Optional By default, the maximum allowed number of continuous real-time accounting failures is five. If five continuous failures occur, the switch cuts down the user connection.

Note

- In an actual network environment, you can specify one server as both the primary and secondary accounting servers, as well as specifying two RADIUS servers as the primary and secondary accounting servers respectively. In addition, because RADIUS adopts different UDP ports to exchange authentication/authorization messages and accounting messages, you must set a port number for accounting different from that set for authentication/authorization.
- With stop-accounting request buffering enabled, the switch first buffers the stop-accounting request that gets no response from the RADIUS accounting server, and then retransmits the request to the RADIUS accounting server until it gets a response, or the maximum number of transmission attempts is reached (in this case, it discards the request).
- You can set the maximum allowed number of continuous real-time accounting failures. If the number of continuously failed real-time accounting requests to the RADIUS server reaches the set maximum number, the switch cuts down the user connection.
- The IP address and port number of the primary accounting server of the default RADIUS scheme "system" are 127.0.0.1 and 1646 respectively.
- Currently, RADIUS does not support the accounting of FTP users.

Configuring Shared Keys for RADIUS Messages

Both RADIUS client and server adopt MD5 algorithm to encrypt RADIUS messages before they are exchanged between the two parties. The two parties verify the validity of the RADIUS messages received from each other by using the shared keys that have been set on them, and can accept and respond to the messages only when both parties have the same shared key.

Follow these steps to configure shared keys for RADIUS messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set a shared key for RADIUS authentication/authorization messages	**key authentication** *string*	Required By default, no shared key is created.
Set a shared key for RADIUS accounting messages	**key accounting** *string*	Required By default, no shared key is created.

Caution

The authentication/authorization shared key and the accounting shared key you set on the switch must be respectively consistent with the shared key on the authentication/authorization server and the shared key on the accounting server.

Configuring the Maximum Number of RADIUS Request Transmission Attempts

The communication in RADIUS is unreliable because this protocol uses UDP packets to carry its data. Therefore, it is necessary for the switch to retransmit a RADIUS request if it gets no response from the RADIUS server after the response timeout timer expires. If the switch gets no answer after it has tried the maximum number of times to transmit the request, the switch considers that the request fails.

Follow these steps to configure the maximum transmission attempts of a RADIUS request:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the maximum number of RADIUS request transmission attempts	**retry** *retry-times*	Optional By default, the system can try three times to transmit a RADIUS request.

Configuring the Type of RADIUS Servers to be Supported

Follow these steps to configure the type of RADIUS servers to be supported:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Configure the type of RADIUS servers to be supported	**server-type** { **extended** | **standard** }	Optional

Note

- If you change the RADIUS server type, the units of data flows sent to RADIUS servers will be restored to the defaults.
- When the third party RADIUS server is used, you can select **standard** or **extended** as the server-type in a RADIUS scheme; when the CAMS server is used, you can select **extended** as the server-type in a RADIUS scheme.

Configuring the Status of RADIUS Servers

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the switch fails to communicate with the primary server due to some server trouble, the switch will turn to the secondary server and exchange messages with the secondary server.

After the primary server remains in the **block** state for a set time (set by the **timer quiet** command), the switch will try to communicate with the primary server again when it receives a RADIUS request. If it finds that the primary server has recovered, the switch immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to **active** while keeping the status of the secondary server unchanged.

When both the primary and secondary servers are in **active** or **block** state, the switch sends messages only to the primary server.

Follow these steps to set the status of RADIUS servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the status of the primary RADIUS authentication/authorization server	**state primary authentication** { **block** | **active** }	Optional By default, the RADIUS servers specified with IP addresses in the RADIUS scheme are all in the **active** state.
Set the status of the primary RADIUS accounting server	**state primary accounting** { **block** | **active** }	

To do…	Use the command…	Remarks
Set the status of the secondary RADIUS authentication/authorization server	**state secondary authentication** { **block** | **active** }	
Set the status of the secondary RADIUS accounting server	**state secondary accounting** { **block** | **active** }	

Configuring the Attributes of Data to be Sent to RADIUS Servers

Follow these steps to configure the attributes of data to be sent to RADIUS servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.
Set the format of the usernames to be sent to RADIUS server	**user-name-format** { **with-domain** | **without-domain** }	Optional By default, the usernames sent from the switch to RADIUS server carry ISP domain names.
Set the units of data flows to RADIUS servers	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega- packet** | **one-packet** }	Optional By default, in a RADIUS scheme, the data unit and packet unit for outgoing RADIUS flows are byte and one-packet respectively.
Set the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets	**calling-station-id mode** { **mode1 | mode2** } { **lowercase | uppercase** }	Optional By default, the MAC address format is XXXX-XXXX-XXXX, in lowercase.
Set the source IP address of outgoing RADIUS messages	RADIUS scheme view **nas-ip** *ip-address*	Optional By default, no source IP address is set; and the IP address of the corresponding outbound interface is used as the source IP address.
	System view **radius nas-ip** *ip-address*	

Note

- Generally, the access users are named in the *userid@isp-name* format. Here, *isp-name* after the "@" character represents the ISP domain name, by which the device determines which ISP domain a user belongs to. However, some old RADIUS servers cannot accept the usernames that carry ISP domain names. In this case, it is necessary to remove domain names from usernames before sending the usernames to RADIUS server. For this reason, the **user-name-format** command is designed for you to specify whether or not ISP domain names are carried in the usernames to be sent to RADIUS server.
- For a RADIUS scheme, if you have specified to remove ISP domain names from usernames, you should not use this RADIUS scheme in more than one ISP domain. Otherwise, such errors may occur: the RADIUS server regards two different users having the same name but belonging to different ISP domains as the same user (because the usernames sent to it are the same).
- In the default RADIUS scheme "system", ISP domain names are removed from usernames by default.
- The purpose of setting the MAC address format of the Calling-Station-Id (Type 31) field in RADIUS packets is to improve the switch's compatibility with different RADIUS servers. This setting is necessary when the format of Calling-Station-Id field recognizable to RADIUS servers is different from the default MAC address format on the switch. For details about field formats recognizable to RADIUS servers, refer to the corresponding RADIUS server manual.

Configuring the Local RADIUS Server

The switch provides the local RADIUS server function (including authentication and authorization), also known as the local RADIUS server function, in addition to RADIUS client service, where separate authentication/authorization server and the accounting server are used for user authentication.

Follow these steps to configure the local RADIUS server function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable UDP ports for local RADIUS services	**local-server enable**	Optional By default, the UDP ports for local RADIUS services are enabled.
Configure the parameters of the local RADIUS server	**local-server nas-ip** *ip-address* **key** *password*	Required By default, a local RADIUS server is configured with an NAS IP address of 127.0.0.1.

Caution

- If you adopt the local RADIUS server function, the UDP port number of the authentication/authorization server must be 1645, the UDP port number of the accounting server must be 1646, and the IP addresses of the servers must be set to the addresses of this switch.
- The message encryption key set by the **local-server nas-ip** *ip-address* **key** *password* command must be identical with the authentication/authorization message encryption key set by the **key authentication** command in the RADIUS scheme view of the RADIUS scheme on the specified NAS that uses this switch as its authentication server.
- The switch supports IP addresses and shared keys for up to 16 network access servers (NAS). That is, when acting as the local RADIUS server, the switch can provide authentication service to up to 16 network access servers (including the switch itself) at the same time.
- When acting as the local RADIUS server, the switch does not support EAP authentication (that is you cannot set the 802.1x authentication method as **eap** by using the **dot1x authentication-method eap** command).

Configuring Timers for RADIUS Servers

After sending out a RADIUS request (authentication/authorization request or accounting request) to a RADIUS server, the switch waits for a response from the server. The maximum time that the switch can wait for the response is called the response timeout time of RADIUS servers, and the corresponding timer in the switch system is called the response timeout timer of RADIUS servers. If the switch gets no answer within the response timeout time, it needs to retransmit the request to ensure that the user can obtain RADIUS service.

For the primary and secondary servers (authentication/authorization servers, or accounting servers) in a RADIUS scheme:

When the switch fails to communicate with the primary server due to some server trouble, the switch will turn to the secondary server and exchange messages with the secondary server.

After the primary server remains in the **block** state for a specific time (set by the **timer quiet** command), the switch will try to communicate with the primary server again when it has a RADIUS request. If it finds that the primary server has recovered, the switch immediately restores the communication with the primary server instead of communicating with the secondary server, and at the same time restores the status of the primary server to **active** while keeping the status of the secondary server unchanged.

To control the interval at which users are charged in real time, you can set the real-time accounting interval. After the setting, the switch periodically sends online users' accounting information to RADIUS server at the set interval.

Follow these steps to set timers for RADIUS servers:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a RADIUS scheme and enter its view	**radius scheme** *radius-scheme-name*	Required By default, a RADIUS scheme named "system" has already been created in the system.

To do…	Use the command…	Remarks
Set the response timeout time of RADIUS servers	**timer response-timeout** *seconds*	Optional By default, the response timeout time of RADIUS servers is three seconds.
Set the time that the switch waits before it try to re-communicate with primary server and restore the status of the primary server to active	**timer quiet** *minutes*	Optional By default, the switch waits five minutes before it restores the status of the primary server to active.
Set the real-time accounting interval	**timer realtime-accounting** *minutes*	Optional By default, the real-time accounting interval is 12 minutes.

Enabling Sending Trap Message when a RADIUS Server Goes Down

Follow these steps to specify to send trap message when a RADIUS server goes down:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the sending of trap message when a RADIUS server is down	**radius trap** { **authentication-server-down** | **accounting-server-down** }	Optional By default, the switch does not send trap message when a RADIUS server is down.

Note

- This configuration takes effect on all RADIUS schemes.
- The switch considers a RADIUS server as being down if it has tried the configured maximum times to send a message to the RADIUS server but does not receive any response.

Enabling the User Re-Authentication at Restart Function

Note

The user re-authentication at restart function applies only to the environment where the RADIUS authentication/authorization and accounting server is CAMS.

In an environment that a CAMS server is used to implement AAA functions, if the switch reboots after an exclusive user (a user whose concurrent online number is set to 1 on the CAMS) gets authenticated and authorized and begins being charged, the switch will give a prompt that the user has already been

online when the user re-logs into the network before the CAMS performs online user detection, and the user cannot get authenticated. In this case, the user can access the network again only when the CAMS administrator manually removes the user's online information.

The user re-authentication at restart function is designed to resolve this problem. After this function is enabled, every time the switch restarts:

1) The switch generates an Accounting-On message, which mainly contains the following information: NAS-ID, NAS-IP-address (source IP address), and session ID.
2) The switch sends the Accounting-On message to the CAMS at regular intervals.
3) Once the CAMS receives the Accounting-On message, it sends a response to the switch. At the same time it finds and deletes the original online information of the users who were accessing the network through the switch before the restart according to the information (NAS-ID, NAS-IP-address and session ID) contained in the message, and ends the accounting for the users depending on the last accounting update message.
4) Once the switch receives the response from the CAMS, it stops sending Accounting-On messages.
5) If the switch does not receive any response from the CAMS after it has tried the configured maximum number of times to send the Accounting-On message, it will not send the Accounting-On message any more.

Note

The switch can automatically generate the main attributes (NAS-ID, NAS-IP-address and session ID) contained in Accounting-On messages. However, you can also manually configure the NAS-IP-address with the **nas-ip** command. If you choose to manually configure the attribute, be sure to configure an appropriate valid IP address. If this attribute is not configured, the switch will automatically choose the IP address of a VLAN interface as the NAS-IP-address.

Follow these steps to enable the user re-authentication at restart function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	—
Enable the user re-authentication at restart function	**accounting-on enable** [**send** *times* | **interval** *interval*]	By default, this function is disabled. If you use this command without any parameter, the system will try at most 15 times to send an Accounting-On message at the interval of three seconds.

Displaying and Maintaining AAA Configuration

Displaying and Maintaining AAA Configuration

To do…	Use the command…	Remarks
Display configuration information about one specific or all ISP domains	**display domain** [*isp-name*]	Available in any view
Display information about user connections	**display connection** [**access-type** { **dot1x** | **mac-authentication** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **vlan** *vlan-id* | **ucibindex** *ucib-index* | **user-name** *user-name*]	
Display information about local users	**display local-user** [**domain** *isp-name* | **idle-cut** { **disable** | **enable** } | **vlan** *vlan-id* | **service-type** { **ftp** | **lan-access** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name*]	

Displaying and Maintaining RADIUS Protocol Configuration

To do…	Use the command…	Remarks
Display RADIUS message statistics about local RADIUS server	**display local-server statistics**	Available in any view
Display configuration information about one specific or all RADIUS schemes	**display radius scheme** [*radius-scheme-name*]	
Display RADIUS message statistics	**display radius statistics**	
Display buffered non-response stop-accounting requests	**display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	
Delete buffered non-response stop-accounting requests	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }	Available in user view
Clear RADIUS message statistics	**reset radius statistics**	

AAA Configuration Examples

Remote RADIUS Authentication of Telnet/SSH Users

Note

The configuration procedure for remote authentication of SSH users by RADIUS server is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for remote authentication.

Network requirements

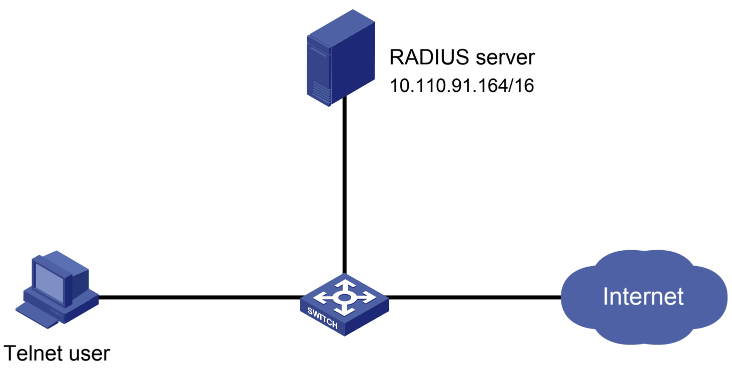
In the network environment shown in Figure 2-1, you are required to configure the switch so that the Telnet users logging into the switch are authenticated by the RADIUS server.

- A RADIUS authentication server with IP address 10.110.91.164 is connected to the switch.
- On the switch, set the shared key it uses to exchange messages with the authentication RADIUS server to **aabbcc**.
- A CAMS server is used as the RADIUS server. You can select **extended** as the server-type in a RADIUS scheme.
- On the RADIUS server, set the shared key it uses to exchange messages with the switch to **aabbcc**, set the authentication port number, and add Telnet usernames and login passwords.

The Telnet usernames added to the RADIUS server must be in the format of *userid@isp-name* if you have configured the switch to include domain names in the usernames to be sent to the RADIUS server in the RADIUS scheme.

Network diagram

Figure 2-1 Remote RADIUS authentication of Telnet users



Configuration procedure

Enter system view.

```
<Sysname> system-view
```

Adopt AAA authentication for Telnet users.

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme
[Sysname-ui-vty0-4] quit
```

Configure an ISP domain.

```
[Sysname] domain cams
[Sysname-isp-cams] access-limit enable 10
```

```
[Sysname-isp-cams] quit
```

Configure a RADIUS scheme.

```
[Sysname] radius scheme cams
[Sysname-radius-cams] accounting optional
[Sysname-radius-cams] primary authentication 10.110.91.164 1812
[Sysname-radius-cams] key authentication aabbcc
[Sysname-radius-cams] server-type Extended
[Sysname-radius-cams] user-name-format with-domain
[Sysname-radius-cams] quit
```

Associate the ISP domain with the RADIUS scheme.

```
[Sysname] domain cams
[Sysname-isp-cams] scheme radius-scheme cams
```

A Telnet user logging into the switch by a name in the format of *userid* @cams belongs to the cams domain and will be authenticated according to the configuration of the cams domain.

Local Authentication of FTP/Telnet Users

Note

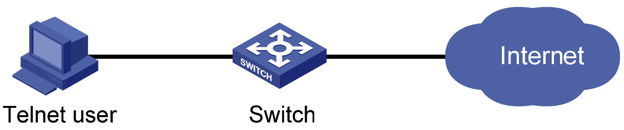
The configuration procedure for local authentication of FTP users is similar to that for Telnet users. The following text only takes Telnet users as example to describe the configuration procedure for local authentication.

Network requirements

In the network environment shown in Figure 2-2, you are required to configure the switch so that the Telnet users logging into the switch are authenticated locally.

Network diagram

Figure 2-2 Local authentication of Telnet users



Configuration procedure

Method 1: Using local authentication scheme.

Enter system view.

```
<Sysname> system-view
```

Adopt AAA authentication for Telnet users.

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme
```

```
[Sysname-ui-vty0-4] quit
```

Create and configure a local user named telnet.

```
[Sysname] local-user telnet
[Sysname-luser-telnet] service-type telnet
[Sysname-luser-telnet] password simple aabbcc
[Sysname-luser-telnet] quit
```

Configure an authentication scheme for the default “system” domain.

```
[Sysname] domain system
[Sysname-isp-system] scheme local
```

A Telnet user logging into the switch with the name telnet@system belongs to the "system" domain and will be authenticated according to the configuration of the "system" domain.

Method 2: using local RADIUS server

This method is similar to the remote authentication method described in Remote RADIUS Authentication of Telnet/SSH Users. However, you need to:

- Change the server IP address, and the UDP port number of the authentication server to 127.0.0.1, and 1645 respectively in the configuration step "Configure a RADIUS scheme" in Remote RADIUS Authentication of Telnet/SSH Users.
- Enable the local RADIUS server function, set the IP address and shared key for the network access server to 127.0.0.1 and aabbcc, respectively.
- Configure local users.

Troubleshooting AAA

Troubleshooting RADIUS Configuration

The RADIUS protocol operates at the application layer in the TCP/IP protocol suite. This protocol prescribes how the switch and the RADIUS server of the ISP exchange user information with each other.

Symptom 1: User authentication/authorization always fails.

Possible reasons and solutions:

- The username is not in the userid@isp-name or *userid.isp-name* format, or the default ISP domain is not correctly specified on the switch — Use the correct username format, or set a default ISP domain on the switch.
- The user is not configured in the database of the RADIUS server — Check the database of the RADIUS server, make sure that the configuration information about the user exists.
- The user input an incorrect password — Be sure to input the correct password.
- The switch and the RADIUS server have different shared keys — Compare the shared keys at the two ends, make sure they are identical.
- The switch cannot communicate with the RADIUS server (you can determine by pinging the RADIUS server from the switch) — Take measures to make the switch communicate with the RADIUS server normally.

Symptom 2: RADIUS packets cannot be sent to the RADIUS server.

Possible reasons and solutions:

- The communication links (physical/link layer) between the switch and the RADIUS server is disconnected/blocked — Take measures to make the links connected/unblocked.

- None or incorrect RADIUS server IP address is set on the switch — Be sure to set a correct RADIUS server IP address.
- One or all AAA UDP port settings are incorrect — Be sure to set the same UDP port numbers as those on the RADIUS server.

Symptom 3: The user passes the authentication and gets authorized, but the accounting information cannot be transmitted to the RADIUS server.

Possible reasons and solutions:

- The accounting port number is not properly set — Be sure to set a correct port number for RADIUS accounting.
- The switch requests that both the authentication/authorization server and the accounting server use the same device (with the same IP address), but in fact they are not resident on the same device — Be sure to configure the RADIUS servers on the switch according to the actual situation.

3 EAD Configuration

Introduction to EAD

Endpoint Admission Defense (EAD) is an attack defense solution. Using this solution, you can enhance the active defense capability of network endpoints, prevents viruses and worms from spreading on the network, and protects the entire network by limiting the access rights of insecure endpoints.

With the cooperation of switch, AAA sever, security policy server and security client, EAD is able to evaluate the security compliance of network endpoints and dynamically control their access rights.

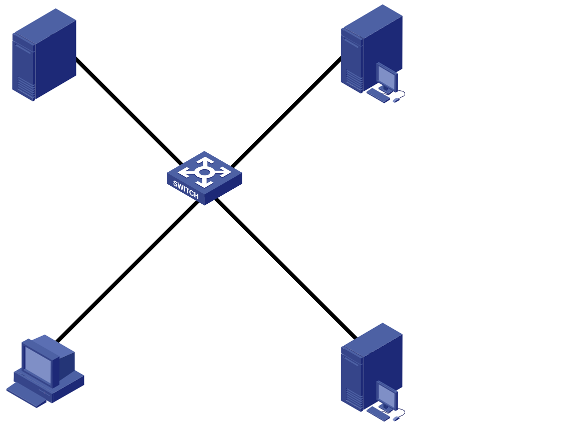
With EAD, a switch:

- Verifies the validity of the session control packets it receives according to the source IP addresses of the packets: It regards only those packets sourced from authentication or security policy server as valid.
- Dynamically adjusts the VLAN, rate and packet scheduling priority for user terminals according to session control packets, whereby to control the access rights of users dynamically.

Typical Network Application of EAD

EAD checks the security status of users before they can access the network, and forcibly implements user access control policies according to the check results. In this way, it can isolate the users that are not compliant with security standard and force these users to update their virus databases and install system patches. Figure 3-1 shows a typical network application of EAD.

Figure 3-1 Typical network application of EAD



EAD Configuration

The EAD configuration includes:

- Configuring the attributes of access users (such as username, user type, and password). For local authentication, you need to configure these attributes on the switch; for remote authentication, you need to configure these attributes on the AAA sever.
- Configuring a RADIUS scheme.
- Configuring the IP address of the security policy server.
- Associating the ISP domain with the RADIUS scheme.

EAD is commonly used in RADIUS authentication environment.

This section mainly describes the configuration of security policy server IP address. For other related configuration, refer to AAA Overview.

Follow these steps to configure EAD:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	—
Configure the RADIUS server type to **extended**	**server-type extended**	Required
Configure the IP address of a security policy server	**security-policy-server** *ip-address*	Required Each RADIUS scheme supports up to eight IP addresses of security policy servers.

EAD Configuration Example

Network requirements

In Figure 3-2:

- A user is connected to Ethernet 1/0/1 on the switch.
- The user adopts 802.1x client supporting EAD extended function.

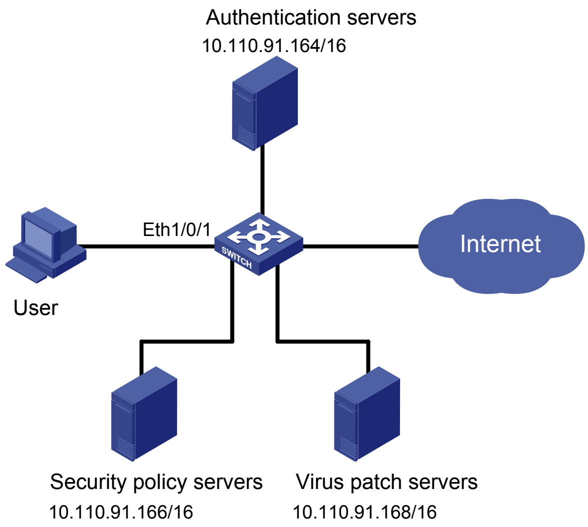
- You are required to configure the switch to use RADIUS server for remote user authentication and use security policy server for EAD control on users.

The following are the configuration tasks:

- Connect the RADIUS authentication server 10.110.91.164 and the switch, and configure the switch to use port number 1812 to communicate with the server.
- Configure the authentication server type to **extended**.
- Configure the encryption password for exchanging messages between the switch and RADIUS server to **expert**.
- Configure the IP address 10.110.91.166 of the security policy server.

Network diagram

Figure 3-2 EAD configuration



Configuration procedure

Configure 802.1x on the switch. Refer to “Configuring 802.1x” in *802.1x and System Guard Configuration*.

Configure a domain.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] quit
```

Configure a RADIUS scheme.

```
[Sysname] radius scheme cams
[Sysname-radius-cams] primary authentication 10.110.91.164 1812
[Sysname-radius-cams] accounting optional
[Sysname-radius-cams] key authentication expert
[Sysname-radius-cams] server-type extended
```

Configure the IP address of the security policy server.

```
[Sysname-radius-cams] security-policy-server 10.110.91.166
```

Associate the domain with the RADIUS scheme.

```
[Sysname-radius-cams] quit
[Sysname] domain system
```

```
[Sysname-isp-system] radius-scheme cams
```

Table of Contents

1 MAC Address Authentication Configuration

When configuring MAC address authentication, go to these sections for information you are interested:

- MAC Address Authentication Overview
- Related Concepts
- Configuring Basic MAC Address Authentication Functions
- MAC Address Authentication Enhanced Function Configuration
- Displaying and Maintaining MAC Address Authentication Configuration
- MAC Address Authentication Configuration Examples

MAC Address Authentication Overview

MAC address authentication provides a way for authenticating users based on ports and MAC addresses, without requiring any client software to be installed on the hosts. Once detecting a new MAC address, it initiates the authentication process. During authentication, the user does not need to enter username or password manually.

For Switch 4500, MAC address authentication can be implemented locally or on a RADIUS server.

After determining the authentication method, users can select one of the following types of user name as required:

- MAC address mode, where the MAC address of a user serves as the user name for authentication.
- Fixed mode, where user names and passwords are configured on a switch in advance. In this case, the user name, the password, and the limits on the total number of user names are the matching criterion for successful authentication. For details, refer to *AAA* of this manual for information about local user attributes.

Performing MAC Address Authentication on a RADIUS Server

When authentications are performed on a RADIUS server, the switch serves as a RADIUS client and completes MAC address authentication in combination of the RADIUS server.

- In MAC address mode, the switch sends the MAC addresses detected to the RADIUS server as both the user names and passwords, or sends the MAC addresses detected to the RADIUS server as the user names and uses the configured fixed password as the password.
- In fixed mode, the switch sends the user name and password previously configured for the user to the RADIUS server for authentication.

A user can access a network upon passing the authentication performed by the RADIUS server.

Performing MAC Address Authentication Locally

When authentications are performed locally, users are authenticated by switches. In this case,

- In MAC address mode, the local user name to be configured is the MAC address of an access user, while the password may be the MAC address of the user or the fixed password configured (which is used depends on your configuration). Hyphens must or must not be included depending on the

format configured with the **mac-authentication authmode usernameasmacaddress usernameformat** command; otherwise, the authentication will fail.

- In fixed mode, all users' MAC addresses are automatically mapped to the configured local passwords and usernames.
- The service type of a local user needs to be configured as lan-access.

Related Concepts

MAC Address Authentication Timers

The following timers function in the process of MAC address authentication:

- Offline detect timer: At this interval, the switch checks to see whether an online user has gone offline. Once detecting that a user becomes offline, the switch sends a stop-accounting notice to the RADIUS server.
- Quiet timer: Whenever a user fails MAC address authentication, the switch does not initiate any MAC address authentication of the user during a period defined by this timer.
- Server timeout timer: During authentication of a user, if the switch receives no response from the RADIUS server in this period, it assumes that its connection to the RADIUS server has timed out and forbids the user from accessing the network.

Quiet MAC Address

When a user fails MAC address authentication, the MAC address becomes a quiet MAC address, which means that any packets from the MAC address will be discarded simply by the switch until the quiet timer expires. This prevents an invalid user from being authenticated repeatedly in a short time.

Caution

If the quiet MAC is the same as the static MAC configured or an authentication-passed MAC, then the quiet function is not effective.

Configuring Basic MAC Address Authentication Functions

Follow these steps to configure basic MAC address authentication functions:

<table>
<tr><th>To do...</th><th colspan="2">Use the command...</th><th>Remarks</th></tr>
<tr><td>Enter system view</td><td colspan="2">system-view</td><td>—</td></tr>
<tr><td>Enable MAC address authentication globally</td><td colspan="2">mac-authentication</td><td>Required
Disabled by default</td></tr>
<tr><td rowspan="3">Enable MAC address authentication for the specified port(s) or the current port</td><td>In system view</td><td>mac-authentication interface interface-list</td><td rowspan="3">Use either method
Disabled by default</td></tr>
<tr><td rowspan="2">In interface view</td><td>interface interface-type interface-number</td></tr>
<tr><td>mac-authentication</td></tr>
</table>

To do...	Use the command...		Remarks
		quit	
Set the user name in MAC address mode for MAC address authentication	**mac-authentication authmode usernameasmacaddress** [**usernameformat** { **with-hyphen** | **without-hyphen** } { **lowercase** | **uppercase** } | **fixedpassword** *password*]		Optional By default, the MAC address of a user is used as the user name.
Set the user name in fixed mode for MAC address authentication	Set the user name in fixed mode for MAC address authentication	**mac-authentication authmode usernamefixed**	Optional By default, the user name is "mac" and no password is configured.
	Configure the user name	**mac-authentication authusername** *username*	
	Configure the password	**mac-authentication authpassword** *password*	
Specify an ISP domain for MAC address authentication	**mac-authentication domain** *isp-name*		Required The default ISP domain (default domain) is used by default.
Configure the MAC address authentication timers	**mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }		Optional The default timeout values are as follows: 300 seconds for offline detect timer; 60 seconds for quiet timer; and 100 seconds for server timeout timer

Caution

- If MAC address authentication is enabled on a port, you cannot configure the maximum number of dynamic MAC address entries for that port (through the **mac-address max-mac-count** command), and vice versa.
- If MAC address authentication is enabled on a port, you cannot configure port security (through the **port-security enable** command) on that port, and vice versa.
- You can configure MAC address authentication on a port before enabling it globally. However, the configuration will not take effect unless MAC address authentication is enabled globally.

MAC Address Authentication Enhanced Function Configuration

MAC Address Authentication Enhanced Function Configuration Task List

Complete the following tasks to configure MAC address authentication enhanced function:

Task	Remarks
Configuring a Guest VLAN	Optional
Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port	Optional

Configuring a Guest VLAN

Note

Different from Guest VLANs described in the *802.1x and System-Guard manual*, Guest VLANs mentioned in this section refer to Guests VLANs dedicated to MAC address authentication.

After completing configuration tasks in Configuring Basic MAC Address Authentication Functions for a switch, this switch can authenticate access users according to their MAC addresses or according to fixed user names and passwords. The switch will not learn MAC addresses of the clients failing in the authentication into its local MAC address table, thus prevent illegal users from accessing the network.

In some cases, if the clients failing in the authentication are required to access some restricted resources in the network (such as the virus library update server), you can use the Guest VLAN.

You can configure a Guest VLAN for each port of the switch. When a client connected to a port fails in MAC address authentication, this port will be added into the Guest VLAN automatically. The MAC address of this client will also be learned into the MAC address table of the Guest VLAN, and thus the user can access the network resources of the Guest VLAN.

After a port is added to a Guest VLAN, the switch will re-authenticate the first access user of this port (namely, the first user whose unicast MAC address is learned by the switch) periodically. If this user passes the re-authentication, this port will exit the Guest VLAN, and thus the user can access the network normally.

Caution

- Guest VLANs are implemented in the mode of adding a port to a VLAN. For example, when multiple users are connected to a port, if the first user fails in the authentication, the other users can access only the contents of the Guest VLAN. The switch will re-authenticate only the first user accessing this port, and the other users cannot be authenticated again. Thus, if more than one client is connected to a port, you cannot configure a Guest VLAN for this port.
- After users that are connected to an existing port failed to pass authentication, the switch adds the port to the Guest VLAN. Therefore, the Guest VLAN can separate unauthenticated users on an access port. When it comes to a trunk port or a hybrid port, if a packet itself has a VLAN tag and be in the VLAN that the port allows to pass, the packet will be forwarded perfectly without the influence of the Guest VLAN. That is, packets can be forwarded to the VLANs other than the Guest VLAN through the trunk port and the hybrid port, even users fail to pass authentication.

Follow these steps to configure a Guest VLAN:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the Guest VLAN for the current port	**mac-authentication guest-vlan** *vlan-id*	Required By default, no Guest VLAN is configured for a port by default.
Return to system view	**quit**	—
Configure the interval at which the switch re-authenticates users in Guest VLANs	**mac-authentication timer guest-vlan-reauth** *interval*	Optional By default, the switch re-authenticates the users in Guest VLANs at the interval of 30 seconds by default.

Caution

- If more than one client are connected to a port, you cannot configure a Guest VLAN for this port.
- When a Guest VLAN is configured for a port, only one MAC address authentication user can access the port. Even if you set the limit on the number of MAC address authentication users to more than one, the configuration does not take effect.
- The undo vlan command cannot be used to remove the VLAN configured as a Guest VLAN. If you want to remove this VLAN, you must remove the Guest VLAN configuration for it. Refer to the VLAN module in this manual for the description on the undo vlan command.
- Only one Guest VLAN can be configured for a port, and the VLAN configured as the Guest VLAN must be an existing VLAN. Otherwise, the Guest VLAN configuration does not take effect. If you want to change the Guest VLAN for a port, you must remove the current Guest VLAN and then configure a new Guest VLAN for this port.
- 802.1x authentication cannot be enabled for a port configured with a Guest VLAN.
- The Guest VLAN function for MAC address authentication does not take effect when port security is enabled.

Configuring the Maximum Number of MAC Address Authentication Users Allowed to Access a Port

You can configure the maximum number of MAC address authentication users for a port in order to control the maximum number of users accessing a port. After the number of access users has exceeded the configured maximum number, the switch will not trigger MAC address authentication for subsequent access users, and thus these subsequent access users cannot access the network normally.

Follow these steps to configure the maximum number of MAC address authentication users allowed to access a port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the maximum number of MAC address authentication users allowed to access a port	**mac-authentication max-auth-num** *user-number*	Required By default, the maximum number of MAC address authentication users allowed to access a port is 256.

Caution

- If both the limit on the number of MAC address authentication users and the limit on the number of users configured in the port security function are configured for a port, the smaller value of the two configured limits is adopted as the maximum number of MAC address authentication users allowed to access this port. Refer to the *Port Security manual* for the description on the port security function.
- You cannot configure the maximum number of MAC address authentication users for a port if any user connected to this port is online.

Displaying and Maintaining MAC Address Authentication Configuration

To do...	Use the command...	Remarks
Display global or on-port information about MAC address authentication	**display mac-authentication** [**interface** *interface-list*]	Available in any view
Clear the statistics of global or on-port MAC address authentication	**reset mac-authentication statistics** [**interface** *interface-type interface-number*]	Available in user view

MAC Address Authentication Configuration Examples

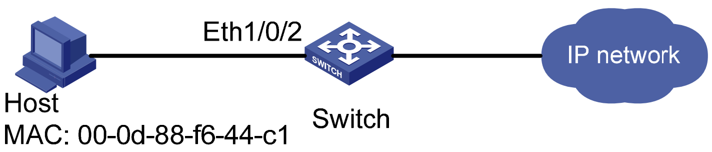
Network requirements

As illustrated in Figure 1-1, a supplicant is connected to the switch through port Ethernet 1/0/2.

- MAC address authentication is required on port Ethernet 1/0/2 to control user access to the Internet.
- All users belong to domain aabbcc.net. The authentication performed is locally and the MAC address of the PC (00-0d-88-f6-44-c1) is used as both the user name and password.

Network Diagram

Figure 1-1 Network diagram for MAC address authentication configuration



Configuration Procedure

Enable MAC address authentication on port Ethernet 1/0/2.

```
<Sysname> system-view
[Sysname] mac-authentication interface Ethernet 1/0/2
```

Set the user name in MAC address mode for MAC address authentication, requiring hyphened lowercase MAC addresses as the usernames and passwords.

```
[Sysname] mac-authentication authmode usernameasmacaddress usernameformat with-hyphen lowercase
```

Add a local user.

- Specify the user name and password.

```
[Sysname] local-user 00-0d-88-f6-44-c1
[Sysname-luser-00-0d-88-f6-44-c1] password simple 00-0d-88-f6-44-c1
```

- Set the service type to **lan-access**.

```
[Sysname-luser-00-0d-88-f6-44-c1] service-type lan-access
[Sysname-luser-00-0d-88-f6-44-c1] quit
```

Add an ISP domain named aabbcc.net.

```
[Sysname] domain aabbcc.net
New Domain added.
```

Specify to perform local authentication.

```
[Sysname-isp-aabbcc.net] scheme local
[Sysname-isp-aabbcc.net] quit
```

Specify aabbcc.net as the ISP domain for MAC address authentication

```
[Sysname] mac-authentication domain aabbcc.net
```

Enable MAC address authentication globally (This is usually the last step in configuring access control related features. Otherwise, a user may be denied of access to the networks because of incomplete configuaration.)

```
[Sysname] mac-authentication
```

After doing so, your MAC address authentication configuration will take effect immediately. Only users with the MAC address of 00-0d-88-f6-44-c1 are allowed to access the Internet through port Ethernet 1/0/2.

Table of Contents

1 ARP Configuration

When configuring ARP, go to these sections for information you are interested in:

Introduction to ARP

ARP Function

Address Resolution Protocol (ARP) is used to resolve an IP address into a data link layer address.

An IP address is the address of a host at the network layer. To send a network layer packet to a destination host, the device must know the data link layer address (MAC address, for example) of the destination host or the next hop. To this end, the IP address must be resolved into the corresponding data link layer address.

Note

Unless otherwise stated, a data link layer address in this chapter refers to a 48-bit Ethernet MAC address.

ARP Message Format

ARP messages are classified as ARP request messages and ARP reply messages. Figure 1-1 illustrates the format of these two types of ARP messages.

- As for an ARP request, all the fields except the hardware address of the receiver field are set. The hardware address of the receiver is what the sender requests for.
- As for an ARP reply, all the fields are set.

Figure 1-1 ARP message format

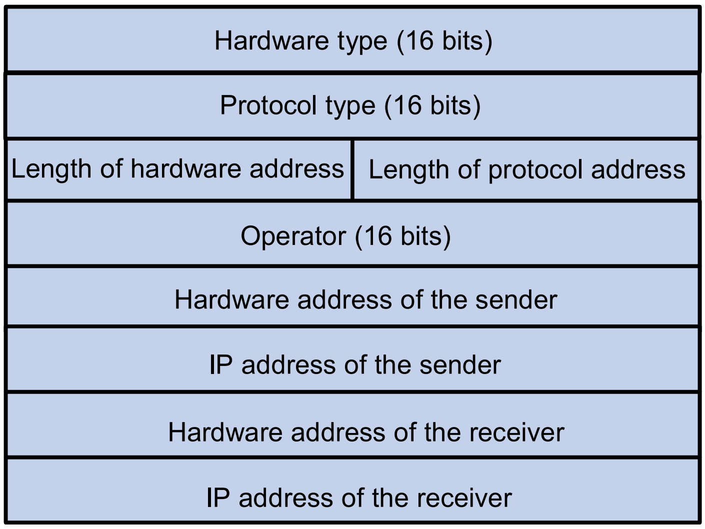


Table 1-1 describes the fields of an ARP packet.

Table 1-1 Description on the fields of an ARP packet

Field	Description
Hardware Type	Type of the hardware interface. Refer to Table 1-2 for the information about the field values.
Protocol type	Type of protocol address to be mapped. 0x0800 indicates an IP address.
Length of hardware address	Hardware address length (in bytes)
Length of protocol address	Protocol address length (in bytes)
Operator	Indicates the type of a data packets, which can be: 1: ARP request packets 2: ARP reply packets 3: RARP request packets 4: RARP reply packets
Hardware address of the sender	Hardware address of the sender
IP address of the sender	IP address of the sender
Hardware address of the receiver	For an ARP request packet, this field is null. For an ARP reply packet, this field carries the hardware address of the receiver.
IP address of the receiver	IP address of the receiver

Table 1-2 Description on the values of the hardware type field

Value	Description
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET (Token Ring)

Value	Description
5	Chaos
6	IEEE802.X
7	ARC network

ARP Table

In an Ethernet, the MAC addresses of two hosts must be available for the two hosts to communicate with each other. Each host in an Ethernet maintains an ARP table, where the latest used IP address-to-MAC address mapping entries are stored. S4500 series Ethernet switches provide the **display arp** command to display the information about ARP mapping entries.

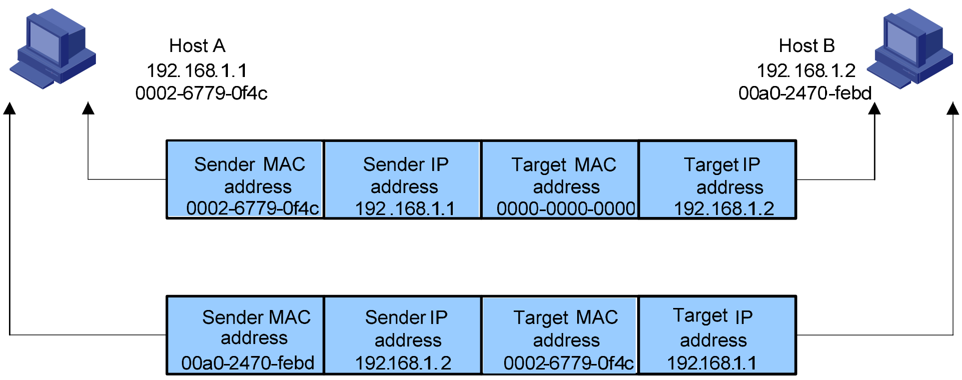
ARP entries in an S4500 series Ethernet switch can either be static entries or dynamic entries, as described in Table 1-3.

Table 1-3 ARP entries

ARP entry	Generation Method	Maintenance Mode
Static ARP entry	Manually configured	Manual maintenance
Dynamic ARP entry	Dynamically generated	ARP entries of this type age with time. The aging period is set by the ARP aging timer.

ARP Process

Figure 1-2 ARP process



Suppose that Host A and Host B are on the same subnet and that Host A sends a message to Host B. The resolution process is as follows:

1) Host A looks in its ARP mapping table to see whether there is an ARP entry for Host B. If Host A finds it, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame and sends the frame to Host B.
2) If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request, in which the source IP address and source MAC address are respectively the IP address and MAC address of Host A and the destination IP address and MAC address are respectively the IP address of Host B and an all-zero MAC address. Because the ARP request is sent in broadcast

mode, all hosts on this subnet can receive the request, but only the requested host (namely, Host B) will process the request.

3) Host B compares its own IP address with the destination IP address in the ARP request. If they are the same, Host B saves the source IP address and source MAC address into its ARP mapping table, encapsulates its MAC address into an ARP reply, and unicasts the reply to Host A.
4) After receiving the ARP reply, Host A adds the MAC address of Host B into its ARP mapping table for subsequent packet forwarding. Meanwhile, Host A encapsulates the IP packet and sends it out.

Usually ARP dynamically implements and automatically seeks mappings from IP addresses to MAC addresses, without manual intervention.

Introduction to Gratuitous ARP

The following are the characteristics of gratuitous ARP packets:

- Both source and destination IP addresses carried in a gratuitous ARP packet are the local addresses, and the source MAC address carried in it is the local MAC addresses.
- If a device finds that the IP addresses carried in a received gratuitous packet conflict with those of its own, it returns an ARP response to the sending device to notify of the IP address conflict.

By sending gratuitous ARP packets, a network device can:

- Determine whether or not IP address conflicts exist between it and other network devices.
- Trigger other network devices to update its hardware address stored in their caches.

With the gratuitous ARP packet learning function enabled:

A device receiving a gratuitous ARP packet adds the information carried in the packet to its own dynamic ARP table if it finds no corresponding ARP entry for the ARP packet exists in the cache.

Periodical sending of gratuitous ARP packets

In an actual network, when the network load or the CPU occupancy of the receiving host is high, ARP packets may be lost or the host may be unable to timely process the ARP packets received. In such a case, the dynamic ARP entries on the receiving host may age out, and the traffic between the host and the sending device will get interrupted before the host learns the MAC address of the sending device again and installs a corresponding entry in the ARP table.

To address this issue, by default, the S4500 series allow VLAN interfaces to send gratuitous ARP packets periodically. That is, as long as a VLAN interface is in the Up state, it sends gratuitous ARP packets at an interval of 30 seconds so that the receiving host can refresh the MAC address of the switch in the ARP table timely, thereby preventing traffic interruption mentioned above.

Introduction to ARP Source MAC Address Consistency Check

An attacker may use the IP or MAC address of another host as the sender IP or MAC address of ARP packets. These ARP packets can cause other network devices to update the corresponding ARP entries incorrectly, thus interrupting network traffic.

To prevent such attacks, you can configure ARP source MAC address consistency check on S4500 series Ethernet switches (operating as gateways). With this function, the device can verify whether an ARP packet is valid by checking the sender MAC address of the ARP packet against the source MAC address in the Ethernet header.

- If they are consistent, the packet passes the check and the switch learns the ARP entry.

- If they are not consistent, the ARP packet is considered invalid and the corresponding ARP entry is not learned.

Configuring ARP

Follow these steps to configure ARP basic functions:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Add a static ARP entry	**arp static** *ip-address mac-address* [*vlan-id interface-type interface-number*]	Optional By default, the ARP mapping table is empty, and entries are created dynamically by ARP.
Configure the ARP aging timer	**arp timer aging** *aging-time*	Optional 20 minutes by default.
Enable the ARP entry checking function (that is, disable the switch from learning ARP entries with multicast MAC addresses)	**arp check enable**	Optional Enabled by default.

Caution

- Static ARP entries are valid as long as the Ethernet switch operates normally. But some operations, such as removing a VLAN, or removing a port from a VLAN, will make the corresponding ARP entries invalid and therefore removed automatically.
- As for the **arp static** command, the value of the *vlan-id* argument must be the ID of an existing VLAN, and the port identified by the *interface-type* and *interface-number* arguments must belong to the VLAN.
- Currently, static ARP entries cannot be configured on the ports of an aggregation group.

Configuring Gratuitous ARP

Follow these steps to configure gratuitous ARP:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the gratuitous ARP packet learning function	**gratuitous-arp-learning enable**	Optional Disabled by default.
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Enable the VLAN interface to send gratuitous ARP packets periodically	**gratuitous-arp period-sending enable**	Optional Enabled by default.

Note

The sending of gratuitous ARP packets is enabled as long as an S4500 switch operates. No command is needed for enabling this function. That is, the device sends gratuitous ARP packets whenever a VLAN interface is enabled (such as when a link is enabled or an IP address is configured for the VLAN interface) or whenever the IP address of a VLAN interface is changed.

Configuring ARP Source MAC Address Consistency Check

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable ARP source MAC address consistency check	**arp anti-attack valid-check enable**	Required Disabled by default.

Displaying and Debugging ARP

To do…	Use the command…	Remarks
Display specific ARP mapping table entries	**display arp** [**static** | **dynamic** | *ip-address*]	Available in any view
Display the ARP mapping entries related to a specified string in a specified way	**display arp** [**dynamic** | **static**] | { **begin** | **include** | **exclude** } *regular-expression*	
Display the number of the ARP entries of a specified type	**display arp count** [[**dynamic** | **static**] [| { **begin** | **include** | **exclude** } *regular-expression*] | *ip-address*]	
Display the statistics about the untrusted ARP packets dropped by the specified port	**display arp detection statistics interface** *interface-type interface-number*	
Display the setting of the ARP aging timer	**display arp timer aging**	
Clear specific ARP entries	**reset arp** [**dynamic** | **static** | **interface** *interface-type interface-number*]	Available in user view

ARP Configuration Examples

Network requirements

- Disable ARP entry check on the switch.
- Disable VLAN-interface 1 of the switch from sending gratuitous ARP packets periodically.
- Set the aging time for dynamic ARP entries to 10 minutes.
- Add a static ARP entry, with the IP address being 192.168.1.1, the MAC address being 000f-e201-0000, and the outbound port being Ethernet 1/0/10 of VLAN 1.

Configuration procedure

```
<Sysname> system-view
[Sysname] undo arp check enable
[Sysname] interface vlan 1
[Sysname-Vlan-interface1] undo gratuitous-arp period-resending enable
[Sysname-Vlan-interface1] quit
[Sysname] arp timer aging 10
[Sysname] arp static 192.168.1.1 000f-e201-0000 1 Ethernet 1/0/10
```

Table of Contents

1 DHCP Overview

When configuring DHCP, go to these sections for information you are interested in:

- Introduction to DHCP
- DHCP IP Address Assignment
- DHCP Packet Format
- Protocol Specification

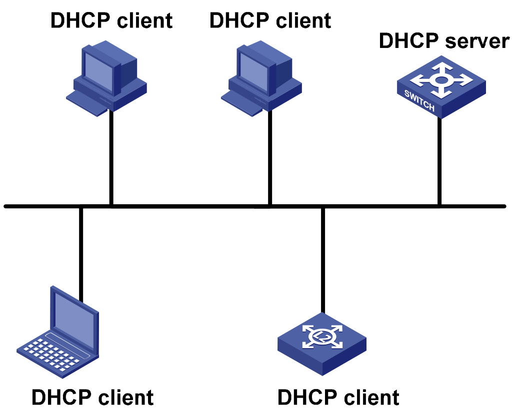
Introduction to DHCP

With networks getting larger in size and more complicated in structure, lack of available IP addresses becomes the common situation the network administrators have to face, and network configuration becomes a tough task for the network administrators. With the emerging of wireless networks and the using of laptops, the position change of hosts and frequent change of IP addresses also require new technology. Dynamic Host Configuration Protocol (DHCP) is developed to solve these issues.

DHCP adopts a client/server model, where the DHCP clients send requests to DHCP servers for configuration parameters; and the DHCP servers return the corresponding configuration information such as IP addresses to implement dynamic allocation of network resources.

A typical DHCP application includes one DHCP server and multiple clients (such as PCs and laptops), as shown in Figure 1-1.

Figure 1-1 Typical DHCP application



DHCP IP Address Assignment

IP Address Assignment Policy

Currently, DHCP provides the following three IP address assignment policies to meet the requirements of different clients:

- Manual assignment. The administrator configures static IP-to-MAC bindings for some special clients, such as a WWW server. Then the DHCP server assigns these fixed IP addresses to the clients.

- Automatic assignment. The DHCP server assigns IP addresses to DHCP clients. The IP addresses will be occupied by the DHCP clients permanently.
- Dynamic assignment. The DHCP server assigns IP addresses to DHCP clients for predetermined period of time. In this case, a DHCP client must apply for an IP address again at the expiration of the period. This policy applies to most clients.

Obtaining IP Addresses Dynamically

A DHCP client undergoes the following four phases to dynamically obtain an IP address from a DHCP server:

1) Discover: In this phase, the DHCP client tries to find a DHCP server by broadcasting a DHCP-DISCOVER packet.
2) Offer: In this phase, the DHCP server offers an IP address. After the DHCP server receives the DHCP-DISCOVER packet from the DHCP client, it chooses an unassigned IP address from the address pool according to the priority order of IP address assignment and then sends the IP address and other configuration information together in a DHCP-OFFER packet to the DHCP client. The sending mode is decided by the flag filed in the DHCP-DISCOVER packet, refer to section DHCP Packet Format for details.
3) Select: In this phase, the DHCP client selects an IP address. If more than one DHCP server sends DHCP-OFFER packets to the DHCP client, the DHCP client only accepts the DHCP-OFFER packet that first arrives, and then broadcasts a DHCP-REQUEST packet containing the assigned IP address carried in the DHCP-OFFER packet.
4) Acknowledge: In this phase, the DHCP servers acknowledge the IP address. Upon receiving the DHCP-REQUEST packet, only the selected DHCP server returns a DHCP-ACK packet to the DHCP client to confirm the assignment of the IP address to the client, or returns a DHCP-NAK packet to refuse the assignment of the IP address to the client. When the client receives the DHCP-ACK packet, it broadcasts an ARP packet with the assigned IP address as the destination address to detect the assigned IP address, and uses the IP address only if it does not receive any response within a specified period.

Note

- After the client receives the DHCP-ACK message, it will probe whether the IP address assigned by the server is in use by broadcasting a gratuitous ARP packet. If the client receives no response within specified time, the client can use this IP address. Otherwise, the client sends a DHCP-DECLINE message to the server and requests an IP address again.
- If there are multiple DHCP servers, IP addresses offered by other DHCP servers are assignable to other clients.

Updating IP Address Lease

After a DHCP server dynamically assigns an IP address to a DHCP client, the IP address keeps valid only within a specified lease time and will be reclaimed by the DHCP server when the lease expires. If the DHCP client wants to use the IP address for a longer time, it must update the IP lease.

By default, a DHCP client updates its IP address lease automatically by unicasting a DHCP-REQUEST packet to the DHCP server when half of the lease time elapses. The DHCP server responds with a DHCP-ACK packet to notify the DHCP client of a new IP lease if the server can assign the same IP address to the client. Otherwise, the DHCP server responds with a DHCP-NAK packet to notify the DHCP client that the IP address will be reclaimed when the lease time expires.

If the DHCP client fails to update its IP address lease when half of the lease time elapses, it will update its IP address lease by broadcasting a DHCP-REQUEST packet to the DHCP servers again when seven-eighths of the lease time elapses. The DHCP server performs the same operations as those described above.

DHCP Packet Format

DHCP has eight types of packets. They have the same format, but the values of some fields in the packets are different. The DHCP packet format is based on that of the BOOTP packets. The following figure describes the packet format (the number in the brackets indicates the field length, in bytes):

Figure 1-2 DHCP packet format

The fields are described as follows:

- op: Operation types of DHCP packets, 1 for request packets and 2 for response packets.
- htype, hlen: Hardware address type and length of the DHCP client.
- hops: Number of DHCP relay agents which a DHCP packet passes. For each DHCP relay agent that the DHCP request packet passes, the field value increases by 1.
- xid: Random number that the client selects when it initiates a request. The number is used to identify an address-requesting process.
- secs: Elapsed time after the DHCP client initiates a DHCP request.
- flags: The first bit is the broadcast response flag bit, used to identify that the DHCP response packet is a unicast (set to 0) or broadcast (set to 1). Other bits are reserved.
- ciaddr: IP address of a DHCP client.
- yiaddr: IP address that the DHCP server assigns to a client.
- siaddr: IP address of the DHCP server.
- giaddr: IP address of the first DHCP relay agent that the DHCP client passes after it sent the request packet.
- chaddr: Hardware address of the DHCP client.
- sname: Name of the DHCP server.

- file: Path and name of the boot configuration file that the DHCP server specifies for the DHCP client.
- option: Optional variable-length fields, including packet type, valid lease time, IP address of a DNS server, and IP address of the WINS server.

Protocol Specification

Protocol specifications related to DHCP include:

- RFC2131: Dynamic Host Configuration Protocol
- RFC2132: DHCP Options and BOOTP Vendor Extensions
- RFC1542: Clarifications and Extensions for the Bootstrap Protocol
- RFC3046: DHCP Relay Agent Information option

2 DHCP Relay Agent Configuration

When configuring the DHCP relay agent, go to these sections for information you are interested in:

Note

Currently, the interface-related DHCP relay agent configurations can only be made on VLAN interfaces.

Introduction to DHCP Relay Agent

Usage of DHCP Relay Agent

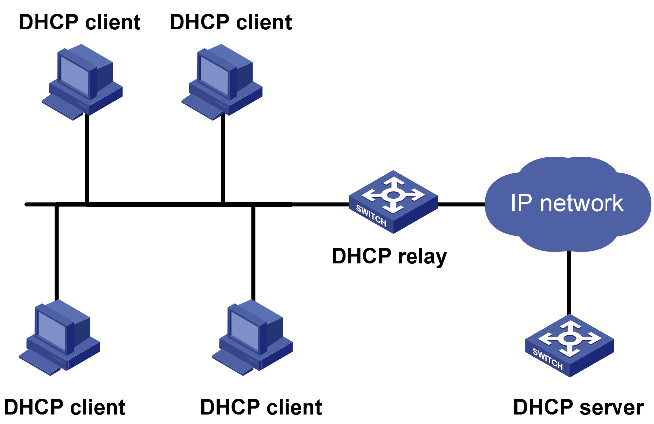
Since the packets are broadcasted in the process of obtaining IP addresses, DHCP is only applicable to the situation that DHCP clients and DHCP servers are in the same network segment, that is, you need to deploy at least one DHCP server for each network segment, which is far from economical.

DHCP relay agent is designed to address this problem. It enables DHCP clients in a subnet to communicate with the DHCP server in another subnet so that the DHCP clients can obtain IP addresses. In this case, the DHCP clients in multiple networks can use the same DHCP server, which can decrease your cost and provide a centralized administration.

DHCP Relay Agent Fundamentals

Figure 2-1 illustrates a typical DHCP relay agent application.

Figure 2-1 Typical DHCP relay agent application



In the process of dynamic IP address assignment through the DHCP relay agent, the DHCP client and DHCP server interoperate with each other in a similar way as they do without the DHCP relay agent. The following sections only describe the forwarding process of the DHCP relay agent. For the interaction process of the packets, see section Obtaining IP Addresses Dynamically.

1) After receiving the DHCP-DISCOVER or DHCP-REQUEST broadcast from the client, the network device providing the DHCP relay agent function unicasts the message to the designated DHCP server based on the configuration.
2) The DHCP server selects an IP address and other parameters and sends the configuration information to the DHCP relay agent that relays the information to the client (the sending mode is decided by the flag filed in the client's DHCP-DISCOVER packet, refer to section DHCP Packet Format for details).

Option 82 Support on DHCP Relay Agent

Introduction to Option 82

Option 82 is the relay agent information option in the DHCP message. It records the location information of the DHCP client. With this option, the administrator can locate the DHCP client to further implement security control and accounting. The Option 82 supporting server can also use such information to define individual assignment policies of IP address and other parameters for the clients.

Option 82 involves at most 255 sub-options. If Option 82 is defined, at least one sub-option must be defined. Currently the DHCP relay agent supports two sub-options: sub-option 1 (circuit ID sub-option) and sub-option 2 (remote ID sub-option).

Padding content of Option 82

Option 82 has no unified definition in RFC 3046. Its padding information varies with vendors. Currently, S4500 Series Ethernet Switches that operate as DHCP relay agents support the extended padding format of Option 82 sub-options. By default, the sub-options of Option 82 are padded as follows, as shown in Figure 2-2 and Figure 2-3. (The content in brackets is the fixed value of each field.)

- sub-option 1: Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client's request.
- sub-option 2: Padded with the bridge MAC address of the DHCP relay agent device that received the client's request.

Figure 2-2 Padding contents for sub-option 1 of Option 82

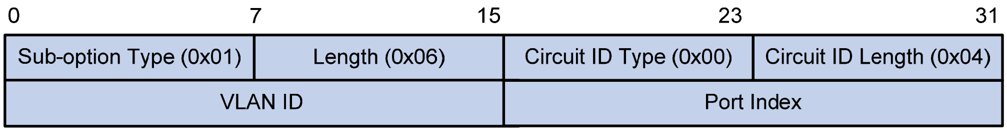
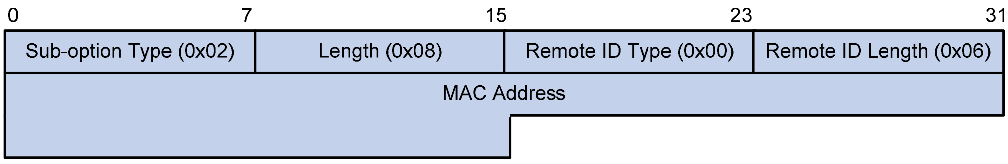


Figure 2-3 Padding contents for sub-option 2 of Option 82



Mechanism of Option 82 supported on DHCP relay agent

The procedure for a DHCP client to obtain an IP address from a DHCP server through a DHCP relay agent is similar to that for the client to obtain an IP address from a DHCP server directly. The following are the mechanism of Option 82 support on DHCP relay agent.

1) Upon receiving a DHCP request, the DHCP relay agent checks whether the packet contains Option 82 and processes the packet accordingly.

- If the request packet contains Option 82, the DHCP relay agent processes the packet depending on the configured strategy (that is, discards the packet, replaces the original Option 82 in the packet with its own, or leaves the original Option 82 unchanged in the packet), and forwards the packet (if not discarded) to the DHCP server.
- If the request packet does not contain Option 82, the DHCP relay agent adds Option 82 to the packet and forwards the packet to the DHCP server.

2) Upon receiving the packet returned from the DHCP server, the DHCP relay agent strips Option 82 from the packet and forwards the packet with the DHCP configuration information to the DHCP client.

Note

Request packets sent by a DHCP client fall into two categories: DHCP-DISCOVER packets and DHCP-REQUEST packets. As DHCP servers coming from different manufacturers process DHCP request packets in different ways (that is, some DHCP servers process Option 82 in DHCP-DISCOVER packets, whereas the rest process Option 82 in DHCP-REQUEST packets), a DHCP relay agent adds Option 82 to both types of packets to accommodate to DHCP servers of different manufacturers.

Configuring the DHCP Relay Agent

Note

If a switch belongs to an XRN fabric, you need to enable the UDP Helper function on it before configuring it as a DHCP relay agent.

DHCP Relay Agent Configuration Task List

Complete the following tasks to configure the DHCP relay agent:

Task	Remarks
Enabling DHCP	Required
Correlating a DHCP Server Group with a Relay Agent Interface	Required
Configuring DHCP Relay Agent Security Functions	Optional
Configuring the DHCP Relay Agent to Support Option 82	Optional

Enabling DHCP

Make sure to enable DHCP before you perform other DHCP relay-related configurations, since other DHCP-related configurations cannot take effect with DHCP disabled.

Follow these steps to enable DHCP:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable DHCP	**dhcp enable**	Required Enabled by default.

Correlating a DHCP Server Group with a Relay Agent Interface

To enhance reliability, you can set multiple DHCP servers on the same network. These DHCP servers form a DHCP server group. When an interface of the relay agent establishes a correlation with the DHCP server group, the interface will forward received DHCP packets to all servers in the server group.

Follow these steps to correlate a DHCP server group with a relay agent interface:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the DHCP server IP address(es) in a specified DHCP server group	**dhcp-server** *groupNo* **ip** *ip-address*&<1-8>	Required By default, no DHCP server IP address is configured in a DHCP server group.
Map an interface to a DHCP server group	**interface** *interface-type interface-number*	Required By default, a VLAN interface is not mapped to any DHCP server group.
	dhcp-server *groupNo*	

Note

To improve security and avoid malicious attack to the unused SOCKETs, S4500 Ethernet switches provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The corresponding implementation is as follows:

- When a VLAN interface is mapped to a DHCP server group with the **dhcp-server** command, the DHCP relay agent is enabled. At the same time, UDP 67 and UDP 68 ports used by DHCP are enabled.
- When the mapping between a VLAN interface and a DHCP server group is removed with the **undo dhcp-server** command, DHCP services are disabled. At the same time, UDP 67 and UDP 68 ports are disabled.

Note

- You can configure up to eight DHCP server IP addresses in a DHCP server group.
- You can map multiple VLAN interfaces to one DHCP server group. But one VLAN interface can be mapped to only one DHCP server group.
- If you execute the **dhcp-server** *groupNo* command repeatedly, the new configuration overwrites the previous one.
- You need to configure the group number specified in the **dhcp-server** *groupNo* command in VLAN interface view by using the command **dhcp-server** *groupNo* **ip** *ip-address&*<1-8> in advance.

Configuring DHCP Relay Agent Security Functions

Configuring address checking

After relaying an IP address from the DHCP server to a DHCP client, the DHCP relay agent can automatically record the client's IP-to-MAC binding and generate a dynamic address entry. It also supports static bindings, which means you can manually configure IP-to-MAC bindings on the DHCP relay agent, so that users can access external network using fixed IP addresses.

The purpose of the address checking function on DHCP relay agent is to prevent unauthorized users from statically configuring IP addresses to access external networks. With this function enabled, a DHCP relay agent inhibits a user from accessing external networks if the IP address configured on the user end and the MAC address of the user end do not match any entries (including the entries dynamically tracked by the DHCP relay agent and the manually configured static entries) in the user address table on the DHCP relay agent.

Follow these steps to configure address checking:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Create a static IP-to-MAC binding	**dhcp-security static** *ip-address mac-address*	Optional Not created by default.
Enter interface view	**interface** *interface-type interface-number*	—
Enable the address checking function	**address-check enable**	Required Disabled by default.

Note

- The **address-check enable** command is independent of other commands of the DHCP relay agent. That is, the invalid address check takes effect when this command is executed, regardless of whether other commands (such as the command to enable DHCP) are used.
- Before executing the **address-check enable** command on the interface connected to the DHCP server, you need to configure the static binding of the IP address to the MAC address of the DHCP server. Otherwise, the DHCP client will fail to obtain an IP address.

Configuring the dynamic client address entry updating function

After relaying an IP address from the DHCP server to the DHCP client, the DHCP relay agent can automatically record the client's IP-to-MAC binding and generate a dynamic address entry. But as a DHCP relay agent does not process DHCP-RELEASE packets, which are sent to DHCP servers by DHCP clients through unicast when the DHCP clients release IP addresses, the user address entries maintained by the DHCP cannot be updated in time. You can solve this problem by enabling the DHCP relay agent handshake function and configuring the dynamic client address entry updating interval.

After the handshake function is enabled, the DHCP relay agent sends the handshake packet (the DHCP-REQUEST packet) periodically to the DHCP server using a client's IP address and its own MAC address.

- If the DHCP relay agent receives the DHCP-ACK packet from the DHCP server, or receives no response from the server within a specified period, the IP address can be assigned. The DHCP relay agent ages out the corresponding entry in the client address table.
- If the DHCP relay agent receives the DHCP-NAK packet from the DHCP server, the lease of the IP address does not expire. The DHCP relay agent does not age out the corresponding entry.

Follow these steps to configure the dynamic user address entry updating function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the DHCP relay agent handshake function	**dhcp relay hand enable**	Optional Enabled by default.
Set the interval at which the DHCP relay agent dynamically updates the client address entries	**dhcp-security tracker** { *interval* | **auto** }	Optional By default, **auto** is adopted, that is, the interval is automatically calculated.

Note

Currently, the DHCP relay agent handshake function on an S4500 series switch can only interoperate with a Windows 2000 DHCP server.

Enabling unauthorized DHCP server detection

If there is an unauthorized DHCP server in the network, when a client applies for an IP address, the unauthorized DHCP server may assign an incorrect IP address to the DHCP client.

With this feature enabled, upon receiving a DHCP message with the siaddr field (IP addresses of the servers offering IP addresses to the client) not being 0 from a client, the DHCP relay agent will record the value of the siaddr field and the receiving interface. The administrator can use this information to check out any DHCP unauthorized servers.

Follow these steps to enable unauthorized DHCP server detection:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable unauthorized DHCP server detection	**dhcp-server detect**	Required Disabled by default.

Note

With the unauthorized DHCP server detection enabled, the relay agent will log all DHCP servers, including authorized ones, and each server is recorded only once until such information is removed and is recorded again. The administrator needs to find unauthorized DHCP servers from the system log information.

Configuring the DHCP Relay Agent to Support Option 82

Prerequisites

Before configuring Option 82 support on a DHCP relay agent, you need to:

- Configure network parameters and relay function of the DHCP relay device.
- Perform assignment strategy-related configurations, such as network parameters of the DHCP server, address pool, and lease time.
- The routes between the DHCP relay agent and the DHCP server are reachable.

Enabling Option 82 support on a DHCP relay agent

Follow these steps to enable Option 82 support on a DHCP relay agent:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Enable Option 82 support on the DHCP relay agent	**dhcp relay information enable**	Required Disabled by default.
Configure the strategy for the DHCP relay agent to process request packets containing Option 82	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	Optional By default, the **replace** strategy is adopted

Note

- By default, with the Option 82 support function enabled on the DHCP relay agent, the DHCP relay agent will adopt the replace strategy to process the request packets containing Option 82. However, if other strategies are configured before, then enabling the 82 support on the DHCP relay agent will not change the configured strategies.
- To enable Option 82, you need to perform the corresponding configuration on the DHCP server and the DHCP relay agent.

Displaying and Maintaining DHCP Relay Agent Configuration

To do…	Use the command…	Remarks
Display the information about a specified DHCP server group	**display dhcp-server** *groupNo*	Available in any view
Display the information about the DHCP server group to which a specified VLAN interface is mapped	**display dhcp-server interface vlan-interface** *vlan-id*	
Display the specified client address entries on the DHCP relay agent	**display dhcp-security** [*ip-address* | **dynamic** | **static** | **tracker**]	
Clear the statistics information of the specified DHCP server group	**reset dhcp-server** *groupNo*	Available in user view

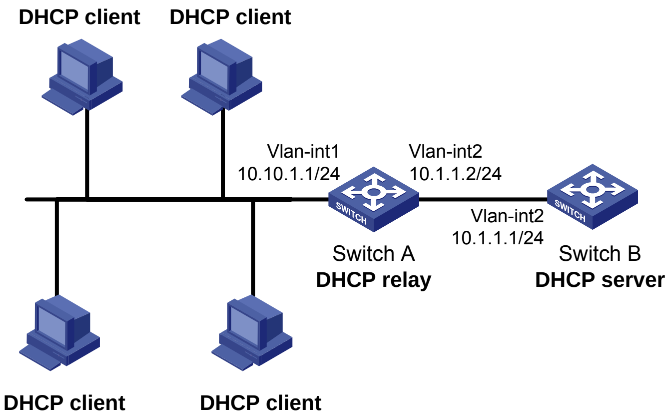
DHCP Relay Agent Configuration Example

Network requirements

VLAN-interface 1 on the DHCP relay agent (Switch A) connects to the network where DHCP clients reside. The IP address of VLAN-interface 1 is 10.10.1.1/24 and IP address of VLAN-interface 2 is 10.1.1.2/24 that communicates with the DHCP server 10.1.1.1/24. As shown in the figure below, Switch A forwards messages between DHCP clients and the DHCP server to assign IP addresses in subnet 10.10.1.0/24 to the clients.

Network diagram

Figure 2-4 Network diagram for DHCP relay agent



Configuration procedure

Create DHCP server group 1 and configure an IP address of 10.1.1.1 for it.

```
<SwitchA> system-view
[SwitchA] dhcp-server 1 ip 10.1.1.1
```

Map VLAN-interface 1 to DHCP server group 1.

```
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] dhcp-server 1
```

Note

- You need to perform corresponding configurations on the DHCP server to enable the DHCP clients to obtain IP addresses from the DHCP server. The DHCP server configurations vary with different DHCP server devices, so the configurations are omitted.
- The DHCP relay agent and DHCP server must be reachable to each other.

Troubleshooting DHCP Relay Agent Configuration

Symptom

A client fails to obtain configuration information through a DHCP relay agent.

Analysis

This problem may be caused by improper DHCP relay agent configuration. When a DHCP relay agent operates improperly, you can locate the problem by enabling debugging and checking the information about debugging and interface state (You can display the information by executing the corresponding display command.)

Solution

- Check if DHCP is enabled on the DHCP server and the DHCP relay agent.

- Check if an address pool that is on the same network segment with the DHCP clients is configured on the DHCP server.
- Check if a reachable route is configured between the DHCP relay agent and the DHCP server.
- Check the DHCP relay agent. Check if the correct DHCP server group is configured on the interface connecting the network segment where the DHCP client resides. Check if the IP address of the DHCP server group is correct.
- If the **address-check enable** command is configured on the interface connected to the DHCP server, verify the DHCP server's IP-to-MAC address binding entry is configured on the DHCP relay agent; otherwise the DHCP client cannot obtain an IP address.

3 DHCP Snooping Configuration

When configuring DHCP snooping, go to these sections for information you are interested in:

DHCP Snooping Overview

Introduction to DHCP Snooping

For the sake of security, the IP addresses used by online DHCP clients need to be tracked for the administrator to verify the corresponding relationship between the IP addresses the DHCP clients obtained from DHCP servers and the MAC addresses of the DHCP clients.

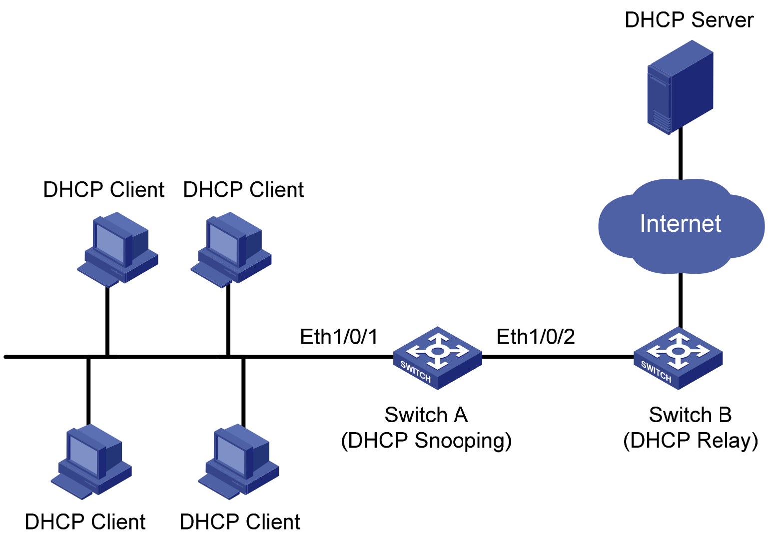
- Switches can track DHCP clients' IP addresses through the security function of the DHCP relay agent operating at the network layer.
- Switches can track DHCP clients' IP addresses through the DHCP snooping function at the data link layer.

When an unauthorized DHCP server exists in the network, a DHCP client may obtains an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, you can specify a port to be a trusted port or an untrusted port by the DHCP snooping function.

- Trusted: A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages to guarantee that DHCP clients can obtain valid IP addresses.
- Untrusted: An untrusted port is connected to an unauthorized DHCP server. The DHCP-ACK or DHCP-OFFER packets received from the port are discarded, preventing DHCP clients from receiving invalid IP addresses.

Figure 3-1 illustrates a typical network diagram for DHCP snooping application, where Switch A is an S4500 series Ethernet switch.

Figure 3-1 Typical network diagram for DHCP snooping application



DHCP snooping listens the following two types of packets to retrieve the IP addresses the DHCP clients obtain from DHCP servers and the MAC addresses of the DHCP clients:

- DHCP-REQUEST packet
- DHCP-ACK packet

Introduction to DHCP-Snooping Option 82

Introduction to Option 82

For details about Option 82, refer to Option 82 Support on DHCP Relay Agent.

Padding content and frame format of Option 82

There is no specification for what should be padded in Option 82. Manufacturers can pad it as required. By default, the sub-options of Option 82 for S4500 Series Ethernet Switches (enabled with DHCP snooping) are padded as follows:

- sub-option 1 (circuit ID sub-option): Padded with the port index (smaller than the physical port number by 1) and VLAN ID of the port that received the client's request.
- sub-option 2 (remote ID sub-option): Padded with the bridge MAC address of the DHCP snooping device that received the client's request.

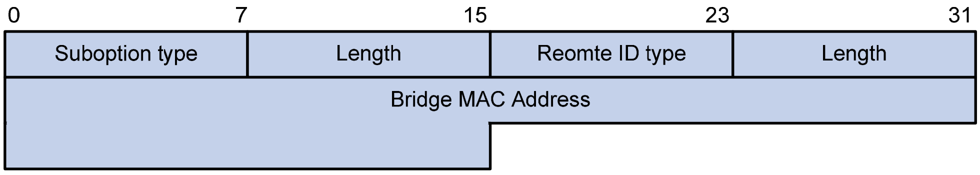
By default, when S4500 Series Ethernet Switches serve as DHCP snooping devices, Option 82 adopts the extended format. Refer to Figure 3-2 and Figure 3-3 for the extended format of the sub-options (with the default padding contents). That is, the circuit ID or remote ID sub-option defines the type and length of a circuit ID or remote ID.

The remote ID type field and circuit ID type field are determined by the option storage format. They are both set to **0** in the case of HEX format and to **1** in the case of ASCII format.

Figure 3-2 Extended format of the circuit ID sub-option

0	7	15	23	31
Suboption type	Length	Circuit ID type	Length	
VLAN ID		Port Index		

Figure 3-3 Extended format of the remote ID sub-option



In practice, some network devices do not support the type and length identifiers of the Circuit ID and Remote ID sub-options. To interwork with these devices, S4500 Series Ethernet Switches support Option 82 in the standard format. Refer to Figure 3-4 and Figure 3-5 for the standard format of the sub-options (with the default padding contents). In the standard format, the Circuit ID or Remote ID sub-option does not contain the two-byte type and length fields of the circuit ID or remote ID.

Figure 3-4 Standard format of the circuit ID sub-option

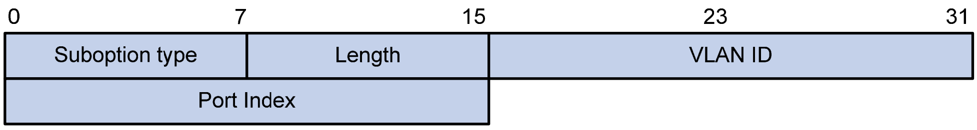
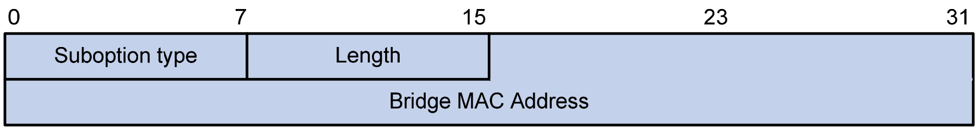


Figure 3-5 Standard format of the remote ID sub-option



Mechanism of DHCP-snooping Option 82

With DHCP snooping and DHCP-snooping Option 82 support enabled, when the DHCP snooping device receives a DHCP client's request containing Option 82, it will handle the packet according to the handling policy and the configured contents in sub-options. For details, see Table 3-1.

Table 3-1 Ways of handling a DHCP packet with Option 82

Handling policy	Sub-option configuration	The DHCP Snooping device will…
Drop	—	Drop the packet.
Keep	—	Forward the packet without changing Option 82.
Replace	Neither of the two sub-options is configured	Forward the packet after replacing the original Option 82 with the default content. The storage format of Option 82 content is the one specified with the **dhcp-snooping information format** command or the default HEX format if this command is not executed.
	Circuit ID sub-option is configured	Forward the packet after replacing the circuit ID sub-option of the original Option 82 with the configured circuit ID sub-option in ASCII format.
	Remote ID sub-option is configured	Forward the packet after replacing the remote ID sub-option of the original Option 82 with the configured remote ID sub-option in ASCII format.

When receiving a DHCP client's request without Option 82, the DHCP snooping device will add the option field with the configured sub-option and then forward the packet. For details, see Table 3-2.

Table 3-2 Ways of handling a DHCP packet without Option 82

Sub-option configuration	The DHCP-Snooping device will …
Neither of the two sub-options is configured.	Forward the packet after adding Option 82 with the default contents. The format of Option 82 is the one specified with the **dhcp-snooping information format** command or the default HEX format if this command is not executed.
Circuit ID sub-option is configured.	Forward the packet after adding Option 82 with the configured circuit ID sub-option in ASCII format.
Remote ID sub-option is configured.	Forward the packet after adding Option 82 with the configured remote ID sub-option in ASCII format.

Note

The circuit ID and remote ID sub-options in Option 82, which can be configured simultaneously or separately, are independent of each other in terms of configuration sequence.

When the DHCP snooping device receives a DHCP response packet from the DHCP server, the DHCP snooping device will delete the Option 82 field, if contained, before forwarding the packet, or will directly forward the packet if the packet does not contain the Option 82 field.

Configuring DHCP Snooping

Configuring DHCP Snooping

Follow these steps to configure DHCP snooping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable DHCP snooping	**dhcp-snooping**	Required By default, the DHCP snooping function is disabled.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Specify the current port as a trusted port	**dhcp-snooping trust**	Required By default, after DHCP snooping is enabled, all ports of a switch are untrusted ports.

Note

- If an S4500 Ethernet switch is enabled with DHCP snooping, the clients connected to it cannot dynamically obtain IP addresses through BOOTP.
- You need to specify the ports connected to the valid DHCP servers as trusted to ensure that DHCP clients can obtain valid IP addresses. The trusted port and the port connected to the DHCP client must be in the same VLAN.
- To enable DHCP snooping on an S4500 switch that belongs to an XRN fabric, do not configure the ports connecting to the DHCP clients and DHCP server to belong to different units of the fabric; otherwise, the switch cannot record DHCP snooping entries although the clients can obtain IP addresses.
- You are not recommended to configure both the DHCP snooping and selective Q-in-Q function on the switch, which may result in the DHCP snooping to function abnormally.

Configuring DHCP Snooping to Support Option 82

Note

Enable DHCP snooping and specify trusted ports on the switch before configuring DHCP snooping to support Option 82.

Complete the following tasks to configure the DHCP snooping to support Option 82:

Task	Remarks
Enabling DHCP-snooping Option 82 support	Required
Configuring a handling policy for DHCP packets with Option 82	Optional
Configuring the storage format of Option 82	Optional
Configuring the circuit ID sub-option	Optional
Configuring the remote ID sub-option	Optional
Configuring the padding format for Option 82	Optional

Enabling DHCP-snooping Option 82 support

Follow these steps to enable DHCP-snooping Option 82 support:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable DHCP-snooping Option 82 support	**dhcp-snooping information enable**	Required Disabled by default.

Configuring a handling policy for DHCP packets with Option 82

Follow these steps to configure a handling policy for DHCP packets with Option 82:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a global handling policy for requests that contain Option 82	**dhcp-snooping information strategy** { **drop** | **keep** | **replace** }	Optional The default handling policy is **replace**.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure a handling policy for requests that contain Option 82 received on the specified interface	**dhcp-snooping information strategy** { **drop** | **keep** | **replace** }	Optional The default policy is **replace**.

Note

If a handling policy is configured on a port, this configuration overrides the globally configured handling policy for requests received on this port, while the globally configured handling policy applies on those ports where a handling policy is not natively configured.

Configuring the storage format of Option 82

S4500 Series Ethernet Switches support the HEX or ASCII format for the Option 82 field.

Follow these steps to configure a storage format for the Option 82 field:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a storage format for the Option 82 field	**dhcp-snooping information format** { **hex | ascii** }	Optional By default, the format is **hex**.

Note

The **dhcp-snooping information format** command applies only to the default content of the Option 82 field. If you have configured the circuit ID or remote ID sub-option, the format of the sub-option is ASCII, instead of the one specified with the **dhcp-snooping information format** command.

Configuring the circuit ID sub-option

Follow these steps to configure the circuit ID sub-option:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the circuit ID sub-option in Option 82	**dhcp-snooping information** [**vlan** *vlan-id*] **circuit-id string** *string*	Optional By default, the circuit ID sub-option contains the VLAN ID and port index related to the port that receives DHCP request packets from DHCP clients

Note

- If you have configured a circuit ID with the **vlan** *vlan-id* argument specified, and the other one without the argument in Ethernet port view, the former circuit ID applies to the DHCP messages from the specified VLAN; while the latter one applies to DHCP messages from other VLANs.
- In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the circuit ID sub-option is subject to the one configured on the primary port.
- The circuit ID sub-option configured on a port will neither be synchronized in the case of port aggregation nor support XRN .

Configuring the remote ID sub-option

You can configure the remote ID sub-option in system view or Ethernet port view:

- In system view, the remote ID takes effect on all interfaces. You can configure Option 82 as the system name (sysname) of the device or any customized character string in the ASCII format.
- In Ethernet port view, the remote ID takes effect only on the current interface. You can configure Option 82 as any customized character string in the ASCII format for different VLANs. That is to say, you can add different configuration rules for packets from different VLANs.

Follow these steps to configure the remote ID sub-option in Option 82:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the remote ID sub-option in system view	**dhcp-snooping information remote-id** { **sysname | string** *string* }	Optional By default, the remote ID sub-option is the MAC address of the DHCP snooping device that received the DHCP client's request.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the remote ID sub-option in Ethernet port view	**dhcp-snooping information** [**vlan** *vlan-id*] **remote-id string** *string*	Optional By default, the remote ID sub-option is the MAC address of the DHCP snooping device that received the client's request.

Note

- If you configure a remote ID sub-option in both system view and on a port, the remote ID sub-option configured on the port applies when the port receives a packet, and the global remote ID applies to other interfaces that have no remote ID sub-option configured.
- If you have configured a remote ID with the **vlan** *vlan-id* argument specified, and the other one without the argument in Ethernet port view, the former remote ID applies to the DHCP messages from the specified VLAN, while the latter one applies to DHCP messages from other VLANs.
- In a port aggregation group, you can use this command to configure the primary and member ports respectively. When Option 82 is added, however, the remote ID is subject to the one configured on the primary port.
- The remote ID configured on a port will neither be synchronized in the case of port aggregation nor support XRN.

Configuring the padding format for Option 82

Follow these steps to configure the padding format for Option 82:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the padding format	**dhcp-snooping information packet-format** { **extended** | **standard** }	Optional By default, the padding format is in extended format.

Displaying and Maintaining DHCP Snooping Configuration

To do…	Use the command…	Remarks
Display the user IP-to-MAC address mapping entries recorded by the DHCP snooping function	**display dhcp-snooping** [**unit** *unit-id*]	Available in any view
Display the (enabled/disabled) state of the DHCP snooping function and the trusted ports	**display dhcp-snooping trust**	

DHCP Snooping Configuration Examples

DHCP-Snooping Option 82 Support Configuration Example

Network requirements

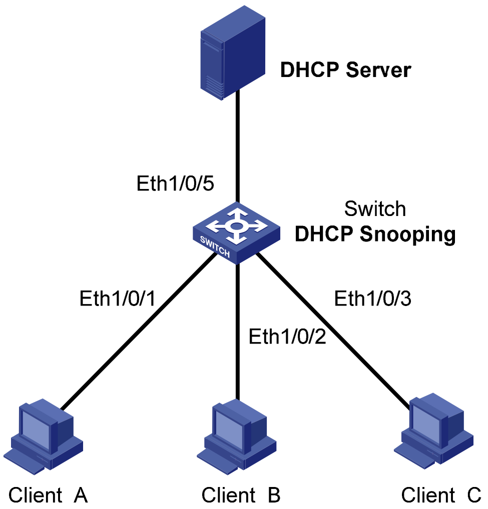
As shown in Figure 3-6, Ethernet 1/0/5 of the switch is connected to the DHCP server, and Ethernet 1/0/1, Ethernet 1/0/2, and Ethernet 1/0/3 are respectively connected to Client A, Client B, and Client C.

- Enable DHCP snooping on the switch.
- Specify Ethernet 1/0/5 on the switch as a trusted port for DHCP snooping.

- Enable DHCP-snooping Option 82 support on the switch and set the remote ID field in Option 82 to the system name of the switch. Set the circuit ID sub-option to **abcd** in DHCP packets from VLAN 1 on Ethernet 1/0/3.

Network diagram

Figure 3-6 Network diagram for DHCP-snooping Option 82 support configuration



Configuration procedure

Enable DHCP snooping on the switch.

```
<Switch> system-view
[Switch] dhcp-snooping
```

Specify Ethernet 1/0/5 as the trusted port.

```
[Switch] interface ethernet 1/0/5
[Switch-Ethernet1/0/5] dhcp-snooping trust
[Switch-Ethernet1/0/5] quit
```

Enable DHCP-snooping Option 82 support.

```
[Switch] dhcp-snooping information enable
```

Set the remote ID sub-option in Option 82 to the system name (sysname) of the DHCP snooping device.

```
[Switch] dhcp-snooping information remote-id sysname
```

Set the circuit ID sub-option in DHCP packets from VLAN 1 to **abcd** on Ethernet 1/0/3.

```
[Switch] interface ethernet 1/0/3
[Switch-Ethernet1/0/3] dhcp-snooping information vlan 1 circuit-id string abcd
```

4 DHCP/BOOTP Client Configuration

When configuring the DHCP/BOOTP client, go to these sections for information you are interested in:

Introduction to DHCP Client

After you specify a VLAN interface as a DHCP client, the device can use DHCP to obtain parameters such as IP address dynamically from the DHCP server, which facilitates user configuration and management.

Refer to Obtaining IP Addresses Dynamically for the process of how a DHCP client dynamically obtains an IP address through DHCP.

For S4500 series Ethernet switches (operating as DHCP clients), the vendor and device information contained in Option 60 of DHCP requests is not configurable; instead, it is populated by the application program of the switches in the format of *vendor-name*. *vendor-name device-model*.

Introduction to BOOTP Client

After you specify an interface as a Bootstrap Protocol (BOOTP) client, the interface can use BOOTP to get information (such as IP address) from the BOOTP server, which simplifies your configuration.

Before using BOOTP, an administrator needs to configure a BOOTP parameter file for each BOOTP client on the BOOTP server. The parameter file contains information such as MAC address and IP address of a BOOTP client. When a BOOTP client sends a request to the BOOTP server, the BOOTP server will search for the BOOTP parameter file and return it to the client.

A BOOTP client dynamically obtains an IP address from a BOOTP server in the following way:

1) The BOOTP client broadcasts a BOOTP request, which contains its own MAC address.
2) The BOOTP server receives the request and searches for the corresponding IP address according to the MAC address of the BOOTP client and sends the information in a BOOTP response to the BOOTP client.
3) The BOOTP client obtains the IP address from the received response.

Note

Because a DHCP server can interact with a BOOTP client, you can use the DHCP server to assign an IP address to the BOOTP client, without needing to configure any BOOTP server.

Configuring a DHCP/BOOTP Client

Follow these steps to configure a DHCP/BOOTP client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface vlan-interface** *vlan-id*	—
Configure the VLAN interface to obtain IP address through DHCP or BOOTP	**ip address** { **bootp-alloc** | **dhcp-alloc** }	Required By default, no IP address is configured for the VLAN interface.

Note

- Currently, an S4500 Ethernet switch functioning as the DHCP client can use an IP address for 24 days at most. That is, the DHCP client can obtain an address lease for no more than 24 days even though the DHCP server offers a longer lease period.
- If a switch belongs to an XRN fabric, you need to enable the UDP Helper function on the switch before configuring its VLAN interfaces to obtain IP addresses through DHCP.

Note

To improve security and avoid malicious attack to the unused SOCKETs, S4500 Ethernet switches provide the following functions:

- UDP 67 and UDP 68 ports used by DHCP are enabled only when DHCP is enabled.
- UDP 67 and UDP 68 ports are disabled when DHCP is disabled.

The specific implementation is:

- Using the **ip address dhcp-alloc** command enables the DHCP client, and UDP port 68.
- Using the **undo ip address dhcp-alloc** command disables the DHCP client, and UDP port 68.

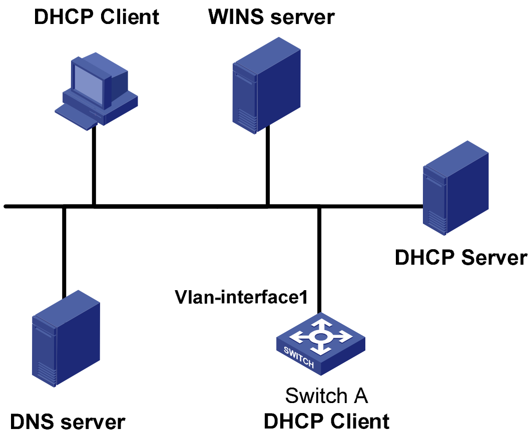
DHCP Client Configuration Example

Network requirements

Using DHCP, VLAN-interface 1 of Switch B is connected to the LAN to obtain an IP address from the DHCP server.

Network diagram

Figure 4-1 A DHCP network



Configuration procedure

The following describes only the configuration on Switch A serving as a DHCP client.

Configure VLAN-interface 1 to dynamically obtain an IP address by using DHCP.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] ip address dhcp-alloc
```

BOOTP Client Configuration Example

Network requirement

Switch B's port belonging to VLAN1 is connected to the LAN. VLAN-interface 1 obtains an IP address from the DHCP server by using BOOTP.

Network diagram

See Figure 4-1.

Configuration procedure

The following describes only the configuration on Switch A serving as a client.

Configure VLAN-interface 1 to dynamically obtain an IP address from the DHCP server.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address bootp-alloc
```

Displaying DHCP/BOOTP Client Configuration

To do…	Use the command…	Remarks
Display related information on a DHCP client	**display dhcp client** [**verbose**]	Optional Available in any view
Display related information on a BOOTP client	**display bootp client** [**interface Vlan-interface** *vlan-id*]	

Table of Contents

1 ACL Configuration

When configuring ACL, go to these sections for information you are interested in:

- ACL Overview
- ACL Configuration Task List
- Displaying and Maintaining ACL Configuration
- Examples for Upper-layer Software Referencing ACLs
- Examples for Applying ACLs to Hardware

ACL Overview

As the network scale and network traffic are increasingly growing, security control and bandwidth assignment play a more and more important role in network management. Filtering data packets can prevent a network from being accessed by unauthorized users efficiently while controlling network traffic and saving network resources. Access Control Lists (ACLs) are often used to filter packets with configured matching rules.

Upon receiving a packet, the switch compares the packet with the rules of the ACL applied on the current port to permit or discard the packet.

The rules of an ACL can be referenced by other functions that need traffic classification, such as QoS.

ACLs classify packets using a series of conditions known as rules. The conditions can be based on source addresses, destination addresses and port numbers carried in the packets.

According to their application purposes, ACLs fall into the following four types.

- Basic ACL. Rules are created based on source IP addresses only.
- Advanced ACL. Rules are created based on the Layer 3 and Layer 4 information such as the source and destination IP addresses, type of the protocols carried by IP, protocol-specific features, and so on.
- Layer 2 ACL. Rules are created based on the Layer 2 information such as source and destination MAC addresses, VLAN priorities, type of Layer 2 protocol, and so on.
- User-defined ACL. An ACL of this type matches packets by comparing the strings retrieved from the packets with specified strings. It defines the byte it begins to perform “and” operation with the mask on the basis of packet headers.

ACL Matching Order

An ACL can contain multiple rules, each of which matches specific type of packets. So the order in which the rules of an ACL are matched needs to be determined.

The rules in an ACL can be matched in one of the following two ways:

- **config**: where rules in an ACL are matched in the order defined by the user.
- **auto**: where rules in an ACL are matched in the order determined by the system, namely the “depth-first” rule (Layer 2 ACLs and user-defined ACLs do not support this feature).

For depth-first rule, there are two cases:

Depth-first match order for rules of a basic ACL

1) Range of source IP address: The smaller the source IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
2) Fragment keyword: A rule with the fragment keyword is prior to others.
3) If the above two conditions are identical, the earlier configured rule applies.

Depth-first match order for rules of an advanced ACL

1) Protocol range: A rule which has specified the types of the protocols carried by IP is prior to others.
2) Range of source IP address: The smaller the source IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
3) Range of destination IP address. The smaller the destination IP address range (that is, the more the number of zeros in the wildcard mask), the higher the match priority.
4) Range of Layer 4 port number, that is, TCP/UDP port number. The smaller the range, the higher the match priority.
5) Number of parameters: the more the parameters, the higher the match priority.

If rule A and rule B are still the same after comparison in the above order, the weighting principles will be used in deciding their priority order. Each parameter is given a fixed weighting value. This weighting value and the value of the parameter itself will jointly decide the final matching order. Involved parameters with weighting values from high to low are **icmp-type**, **established**, **dscp**, **tos**, **precedence**, **fragment**. Comparison rules are listed below.

- The smaller the weighting value left, which is a fixed weighting value minus the weighting value of every parameter of the rule, the higher the match priority.
- If the types of parameter are the same for multiple rules, then the sum of parameters' weighting values of a rule determines its priority. The smaller the sum, the higher the match priority.

Ways to Apply an ACL on a Switch

Being applied to the hardware directly

In the switch, an ACL can be directly applied to hardware for packet filtering and traffic classification. In this case, the rules in an ACL are matched in the order determined by the hardware instead of that defined in the ACL. For Switch 4500 series, the later the rule applies, the higher the match priority.

ACLs are directly applied to hardware when they are used for:

- Implementing QoS
- Filtering the packets to be forwarded

Being referenced by upper-level software

ACLs can also be used to filter and classify the packets to be processed by software. In this case, the rules in an ACL can be matched in one of the following two ways:

- **config**, where rules in an ACL are matched in the order defined by the user.
- **auto**, where the rules in an ACL are matched in the order determined by the system, namely the "depth-first" order (Layer 2 ACLs and user-defined ACLs do not support this feature).

When applying an ACL in this way, you can specify the order in which the rules in the ACL are matched. The match order cannot be modified once it is determined, unless you delete all the rules in the ACL and define the match order.

An ACL can be referenced by upper-layer software:

- Referenced by routing policies
- Used to control Telnet, SNMP and Web login users

Note

- When an ACL is directly applied to hardware for packet filtering, the switch will permit packets if the packets do not match the ACL.
- When an ACL is referenced by upper-layer software to control Telnet, SNMP and Web login users, the switch will deny packets if the packets do not match the ACL.

Types of ACLs Supported by Switch 4500 Series

The following types of ACLs are supported by Switch 4500 series:

- Basic ACL
- Advanced ACL
- Layer 2 ACL
- User-defined ACL

In addition, ACLs defined on Switch 4500 series can be applied to hardware directly or referenced by upper-layer software for packet filtering.

ACL Configuration Task List

Complete the following tasks to configure ACL:

Task	Remarks
Configuring Time Range	Optional
Configuring Basic ACL	Required
Configuring Advanced ACL	Required
Configuring Layer 2 ACL	Required
Configuring User-defined ACL	Required
Applying ACL Rules on Ports	Required
Applying ACL rules to Ports in a VLAN	Required

Configuring Time Range

Time ranges can be used to filter packets. You can specify a time range for each rule in an ACL. A time range-based ACL takes effect only in specified time ranges. Only after a time range is configured and the system time is within the time range, can an ACL rule take effect.

Two types of time ranges are available:

- Periodic time range, which recurs periodically on the day or days of the week.
- Absolute time range, which takes effect only in a period of time and does not recur.

Note

An absolute time range on Switch 4500 Series can be within the range 1970/1/1 00:00 to 2100/12/31 24:00.

Configuration procedure

Follow these steps to configure a time range:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create a time range	**time-range** *time-name* { *start-time* **to** *end-time* *days-of-the-week* [**from** *start-time start-date*] [**to** *end-time end-date*] | **from** *start-time* *start-date* [**to** *end-time end-date*] | **to** *end-time end-date* }	Required

Note that:

- If only a periodic time section is defined in a time range, the time range is active only when the system time is within the defined periodic time section. If multiple periodic time sections are defined in a time range, the time range is active only when the system time is within one of the periodic time sections.
- If only an absolute time section is defined in a time range, the time range is active only when the system time is within the defined absolute time section. If multiple absolute time sections are defined in a time range, the time range is active only when the system time is within one of the absolute time sections.
- If both a periodic time section and an absolute time section are defined in a time range, the time range is active only when the periodic time range and the absolute time range are both matched. Assume that a time range contains an absolute time section ranging from 00:00 January 1, 2004 to 23:59 December 31, 2004, and a periodic time section ranging from 12:00 to 14:00 on every Wednesday. This time range is active only when the system time is within the range from 12:00 to 14:00 on every Wednesday in 2004.
- If the start time is not specified, the time section starts from 1970/1/1 00:00 and ends on the specified end date. If the end date is not specified, the time section starts from the specified start date to 2100/12/31 23:59.

Configuration example

Define a periodic time range that spans from 8:00 to 18:00 on Monday through Friday.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 working-day
[Sysname] display time-range test
Current time is 13:27:32 Apr/16/2005 Saturday

Time-range : test ( Inactive )
 08:00 to 18:00 working-day
```

Define an absolute time range spans from 15:00 1/28/2006 to 15:00 1/28/2008.

```
<Sysname> system-view
[Sysname] time-range test from 15:00 1/28/2006 to 15:00 1/28/2008
[Sysname] display time-range test
Current time is 13:30:32 Apr/16/2005 Saturday

Time-range : test ( Inactive )
 From 15:00 Jan/28/2006 to 15:00 Jan/28/2008
```

Configuring Basic ACL

A basic ACL filters packets based on their source IP addresses.

A basic ACL can be numbered from 2000 to 2999.

Configuration prerequisites

- To configure a time range-based basic ACL rule, you need to create the corresponding time range first. For information about time range configuration, refer to Configuring Time Range.
- The source IP addresses based on which the ACL filters packets are determined.

Configuration procedure

Follow these steps to define a basic ACL rule:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create an ACL and enter basic ACL view	**acl number** *acl-number* [**match-order** { **auto** | **config** }]	Required **config** by default
Define an ACL rule	**rule** [*rule-id*] { **deny** | **permit** } [*rule-string*]	Required For information about *rule-string*, refer to *ACL Command*.
Configure a description string to the ACL	**description** *text*	Optional Not configured by default

Note that:

- With the **config** match order specified for the basic ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the basic ACL, you cannot modify any existent rule; otherwise the system prompts error information.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rule; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
- With the **auto** match order specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.

Configuration example

Configure ACL 2000 to deny packets whose source IP addresses are 192.168.0.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 192.168.0.1 0
```

Display the configuration information of ACL 2000.

```
[Sysname-acl-basic-2000] display acl 2000
Basic ACL  2000, 1 rule
Acl's step is 1
 rule 0 deny source 192.168.0.1 0
```

Configuring Advanced ACL

An advanced ACL can filter packets by their source and destination IP addresses, the protocols carried by IP, and protocol-specific features such as TCP/UDP source and destination ports, ICMP message type and message code.

An advanced ACL can be numbered from 3000 to 3999. Note that ACL 3998 and ACL 3999 cannot be configured because they are reserved for cluster management.

Advanced ACLs support analysis and processing of three packet priority levels: type of service (ToS) priority, IP priority and differentiated services codepoint (DSCP).

Using advanced ACLs, you can define classification rules that are more accurate, more abundant, and more flexible than those defined for basic ACLs.

Configuration prerequisites

- To configure a time range-based advanced ACL rule, you need to create the corresponding time ranges first. For information about of time range configuration, refer to Configuring Time Range.
- The settings to be specified in the rule, such as source and destination IP addresses, the protocols carried by IP, and protocol-specific features, are determined.

Configuration procedure

Follow these steps to define an advanced ACL rule:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create an advanced ACL and enter advanced ACL view	**acl number** *acl-number* [**match-order** { **auto** | **config** }]	Required **config** by default
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } *protocol* [*rule-string*]	Required For information about *protocol* and *rule-string*, refer to *ACL Commands*.
Assign a description string to the ACL rule	**rule** *rule-id* **comment** *text*	Optional No description by default
Assign a description string to the ACL	**description** *text*	Optional No description by default

Note that:

- With the **config** match order specified for the advanced ACL, you can modify any existent rule. The unmodified part of the rule remains. With the **auto** match order specified for the ACL, you cannot modify any existent rule; otherwise the system prompts error information.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.
- If the ACL is created with the **auto** keyword specified, the newly created rules will be inserted in the existent ones by depth-first principle, but the numbers of the existent rules are unaltered.

Configuration example

Configure ACL 3000 to permit the TCP packets sourced from the network 129.9.0.0/16 and destined for the network 202.38.160.0/24 and with the destination port number being 80.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0
0.0.0.255 destination-port eq 80
```

Display the configuration information of ACL 3000.

```
[Sysname-acl-adv-3000] display acl 3000
Advanced ACL  3000, 1 rule
Acl's step is 1
 rule 0 permit tcp source 129.9.0.0 0.0.255.255 destination 202.38.160.0 0.0.0.255
destination-port eq www
```

Configuring Layer 2 ACL

Layer 2 ACLs filter packets according to their Layer 2 information, such as the source and destination MAC addresses, VLAN priority, and Layer 2 protocol types.

A Layer 2 ACL can be numbered from 4000 to 4999.

Configuration prerequisites

- To configure a time range-based Layer 2 ACL rule, you need to create the corresponding time ranges first. For information about time range configuration, refer to Configuring Time Range
- The settings to be specified in the rule, such as source and destination MAC addresses, VLAN priorities, and Layer 2 protocol types, are determined.

Configuration procedure

Follow these steps to define a Layer 2 ACL rule:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create a Layer 2 ACL and enter layer 2 ACL view	**acl number** *acl-number*	Required

To do...	Use the command...	Remarks
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	Required For information about *rule-string*, refer to *ACL Commands*.
Assign a description string to the ACL rule	**rule** *rule-id* **comment** *text*	Optional No description by default
Assign a description string to the ACL	**description** *text*	Optional No description by default

Note that:

- You can modify any existent rule of the Layer2 ACL and the unmodified part of the ACL remains.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

Configuration example

Configure ACL 4000 to deny packets sourced from the MAC address 000d-88f5-97ed, destined for the MAC address 0011-4301-991e, and with their 802.1p priority being 3.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny cos 3 source 000d-88f5-97ed ffff-ffff-ffff dest
0011-4301-991e ffff-ffff-ffff
```

Display the configuration information of ACL 4000.

```
[Sysname-acl-ethernetframe-4000] display acl 4000
Ethernet frame ACL  4000, 1 rule
Acl's step is 1
 rule 0 deny cos excellent-effort source 000d-88f5-97ed ffff-ffff-ffff dest 0011-4301-991e
ffff-ffff-ffff
```

Configuring User-defined ACL

A user-defined ACL filters packets by comparing specific bytes in packet headers with specified string.

A user-defined ACL can be numbered from 5000 to 5999.

Configuration prerequisites

To configure a time range-based user-defined ACL rule, you need to define the corresponding time ranges first. For information about time range configuration, refer to Configuring Time Range.

Configuration procedure

Follow these steps to define a user-defined ACL rule:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Create a user-defined ACL and enter user-defined ACL view	**acl number** *acl-number*	Required
Define an ACL rule	**rule** [*rule-id*] { **permit** | **deny** } [*rule-string rule-mask offset*] &<1-8> [**time-range** *time-name*]	Required For information about *rule-string*, refer to *ACL Commands*.
Define a comment for the ACL rule	**rule** *rule-id* **comment** *text*	Optional No description by default
Define a description for the ACL	**description** *text*	Optional No description by default

Note

When configuring a rule that matches specific fields of packets, take the following two items into account:

- If VLAN-VPN is not enabled, each packet in the switch carries one VLAN tag, which is 4 bytes long.
- If VLAN-VPN is enabled on a port, each packet in the switch carries two VLAN tags, which is 8 bytes long.

Note that:

- You can modify any existent rule of a user-defined ACL. If you modify only the time range and/or action, the unmodified parts of the rule remain the same. If you modify the *rule-string rule-mask offset* combinations, however, the new combinations will replace all of the original ones.
- If you do not specify the *rule-id* argument when creating an ACL rule, the rule will be numbered automatically. If the ACL has no rules, the rule is numbered 0; otherwise, the number of the rule will be the greatest rule number plus one. If the current greatest rule number is 65534, however, the system will display an error message and you need to specify a number for the rule.
- The content of a modified or created rule cannot be identical with the content of any existing rules; otherwise the rule modification or creation will fail, and the system prompts that the rule already exists.

Configuration example

Configure ACL 5000 to deny all TCP packets, provided that VLAN-VPN is not enabled on any port. In the ACL rule, 06 is the TCP protocol number, ff is the mask of the rule, and 27 is the protocol field offset of an internally processed IP packet.

```
<Sysname> system-view
[Sysname] acl number 5000
[Sysname-acl-user-5000] rule deny 06 ff 27
```

Display the configuration information of ACL 5000.

```
[Sysname-acl-user-5000] display acl 5000
User defined ACL  5000, 1 rule
```

```
Acl's step is 1
 rule 0 deny 06 ff 27
```

Applying ACL Rules on Ports

By applying ACL rules on ports, you can filter packets on the corresponding ports.

Configuration prerequisites

You need to define an ACL before applying it on a port. For information about defining an ACL, refer to Configuring Basic ACL, Configuring Advanced ACL, Configuring Layer 2 ACL, and Configuring User-defined ACL.

Configuration procedure

Follow these steps to apply ACL rules on a port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Apply ACL rules on the port	**packet-filter** { **inbound** | **outbound** } *acl-rule*	Required For information about *acl-rule*, refer to *ACL Commands*.

Configuration example

Apply ACL 2000 on Ethernet 1/0/1 to filter inbound packets.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] packet-filter inbound ip-group 2000
```

Applying ACL rules to Ports in a VLAN

By applying ACL rules to ports in a VLAN, you can add filtering of packets on all the ports in the VLAN.

Note:

The ACL rules are only applied to ports that are in the VLAN at the time the **packet-filter vlan** command is executed. In other words:

- A port joining the VLAN later will not use the ACL rules for packet filtering.
- A port leaving the VLAN later will keep using the ACL rules for packet filtering.

Configuration prerequisites

Before applying ACL rules to ports in a VLAN, you need to define the related ACLs. For information about defining an ACL, refer to Configuring Basic ACL, Configuring Advanced ACL, Configuring Layer 2 ACL, and Configuring User-defined ACL.

Configuration procedure

Follow these steps to apply ACL rules to ports in a VLAN:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Apply ACL rules to ports in a VLAN	**packet-filter vlan** *vlan-id* { **inbound** | **outbound** } *acl-rule*	Required For information about *acl-rule*, refer to *ACL Commands*.

Configuration example

Apply ACL 2000 to all ports of VLAN 1 in the inbound direction to filter packets.

```
<Sysname> system-view
[Sysname] packet-filter vlan 1 inbound ip-group 2000
```

Displaying and Maintaining ACL Configuration

To do...	Use the command...	Remarks
Display a configured ACL or all the ACLs	**display acl** { **all** | *acl-number* }	Available in any view
Display a time range or all the time ranges	**display time-range** { **all** | *time-name* }	
Display information about packet filtering	**display packet-filter** { **interface** *interface-type interface-number* | **unitid** *unit-id* }	
Display information about ACL resources	**display drv qacl_resource**	

Examples for Upper-layer Software Referencing ACLs

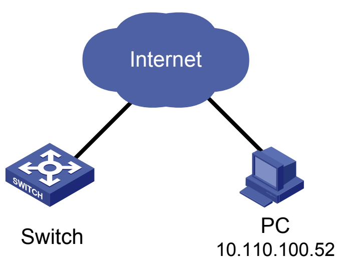
Example for Controlling Telnet Login Users by Source IP

Network requirements

Apply an ACL to permit users with the source IP address of 10.110.100.52 to telnet to the switch.

Network diagram

Figure 1-1 Network diagram for controlling Telnet login users by source IP



Configuration procedure

Define ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] quit
```

Reference ACL 2000 on VTY user interface to control Telnet login users.

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

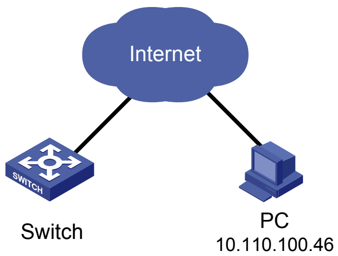
Example for Controlling Web Login Users by Source IP

Network requirements

Apply an ACL to permit Web users with the source IP address of 10.110.100.46 to log in to the switch through HTTP.

Network diagram

Figure 1-2 Network diagram for controlling Web login users by source IP



Configuration procedure

Define ACL 2001.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule 1 permit source 10.110.100.46 0
[Sysname-acl-basic-2001] quit
```

Reference ACL 2001 to control users logging in to the Web server.

```
[Sysname] ip http acl 2001
```

Examples for Applying ACLs to Hardware

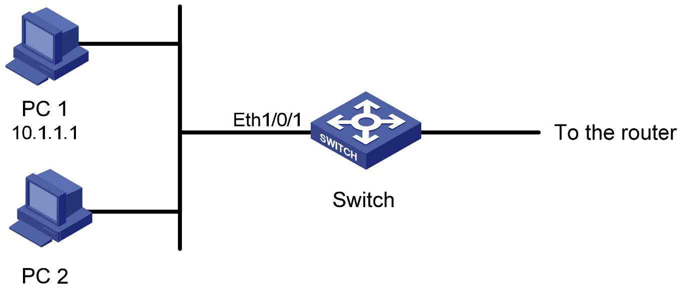
Basic ACL Configuration Example

Network requirements

PC 1 and PC 2 connect to the switch through Ethernet 1/0/1. PC1's IP address is 10.1.1.1. Apply an ACL on Ethernet 1/0/1 to deny packets with the source IP address of 10.1.1.1 from 8:00 to 18:00 everyday.

Network diagram

Figure 1-3 Network diagram for basic ACL configuration



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 daily
```

Define ACL 2000 to filter packets with the source IP address of 10.1.1.1.

```
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 1 deny source 10.1.1.1 0 time-range test
[Sysname-acl-basic-2000] quit
```

Apply ACL 2000 on Ethernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] packet-filter inbound ip-group 2000
```

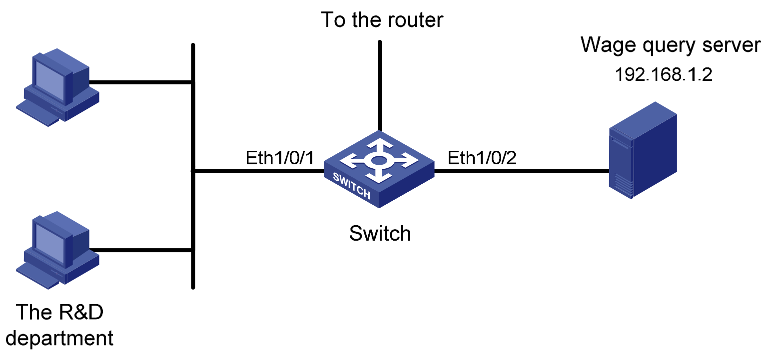
Advanced ACL Configuration Example

Network requirements

Different departments of an enterprise are interconnected through a switch. The IP address of the wage query server is 192.168.1.2. The R&D department is connected to Ethernet 1/0/1 of the switch. Apply an ACL to deny requests from the R&D department and destined for the wage server during the working hours (8:00 to 18:00).

Network diagram

Figure 1-4 Network diagram for advanced ACL configuration



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 working-day
```

Define ACL 3000 to filter packets destined for wage query server.

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range test
[Sysname-acl-adv-3000] quit
```

Apply ACL 3000 on Ethernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] packet-filter inbound ip-group 3000
```

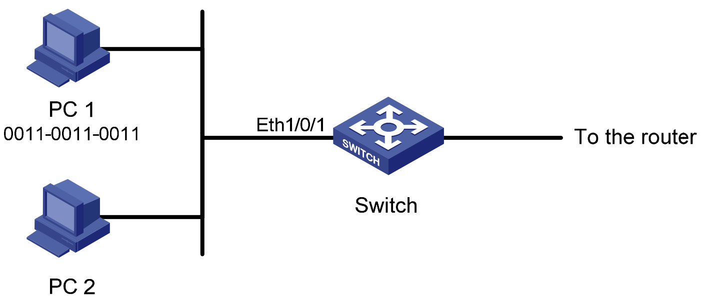
Layer 2 ACL Configuration Example

Network requirements

PC 1 and PC 2 connect to the switch through Ethernet 1/0/1. PC 1's MAC address is 0011-0011-0011. Apply an ACL to filter packets with the source MAC address of 0011-0011-0011 and the destination MAC address of 0011-0011-0012 from 8:00 to 18:00 everyday.

Network diagram

Figure 1-5 Network diagram for Layer 2 ACL



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 daily
```

Define ACL 4000 to filter packets with the source MAC address of 0011-0011-0011 and the destination MAC address of 0011-0011-0012.

```
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule 1 deny source 0011-0011-0011 ffff-ffff-ffff dest
0011-0011-0012 ffff-ffff-ffff time-range test
[Sysname-acl-ethernetframe-4000] quit
```

Apply ACL 4000 on Ethernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] packet-filter inbound link-group 4000
```

User-defined ACL Configuration Example

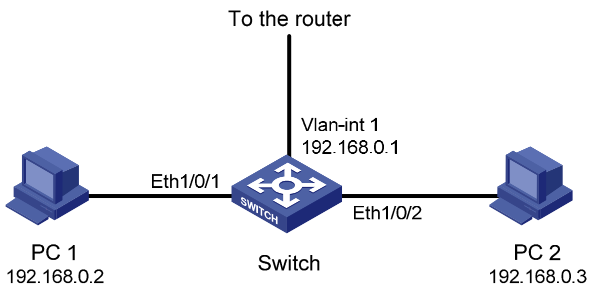
Network requirements

As shown in Figure 1-6, PC 1 and PC 2 are connected to the switch through Ethernet 1/0/1 and Ethernet 1/0/2 respectively. They belong to VLAN 1 and access the Internet through the same gateway, which has an IP address of 192.168.0.1 (the IP address of VLAN-interface 1).

Configure a user-defined ACL to deny all ARP packets from PC 1 that use the gateway IP address as the source address from 8:00 to 18:00 everyday.

Network diagram

Figure 1-6 Network diagram for user-defined ACL



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 everyday.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 daily
```

Define ACL 5000 to deny any ARP packet whose source IP address is 192.168.0.1 from 8:00 to 18:00 everyday (provided that VLAN-VPN is not enabled on any port). In the ACL rule, 0806 is the ARP protocol number, ffff is the mask of the rule, 16 is the protocol type field offset of the internally processed Ethernet frame, c0a80001 is the hexadecimal form of 192.168.0.1, and 32 is the source IP address field offset of the internally processed ARP packet.

```
[Sysname] acl number 5000
[Sysname-acl-user-5000] rule 1 deny 0806 ffff 16 c0a80001 ffffffff 32 time-range test
```

Apply ACL 5000 on Ethernet 1/0/1.

```
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] packet-filter inbound user-group 5000
```

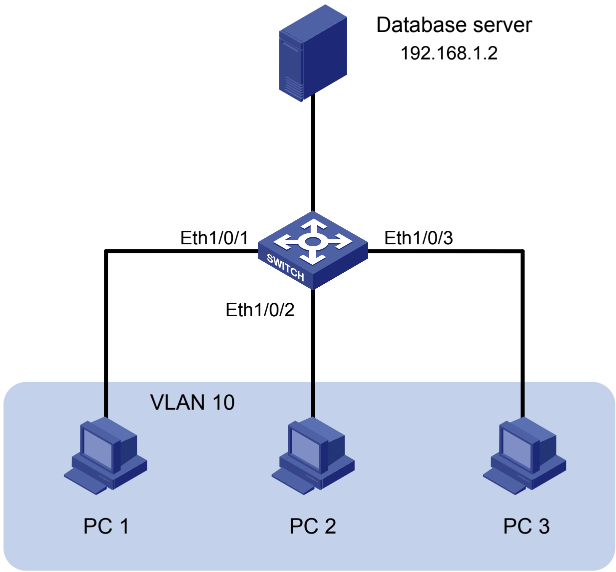
Example for Applying an ACL to a VLAN

Network requirements

PC 1, PC 2 and PC 3 belong to VLAN 10 and connect to the switch through Ethernet 1/0/1, Ethernet 1/0/2 and Ethernet 1/0/3 respectively. The IP address of the database server is 192.168.1.2. Apply an ACL to deny packets from PCs in VLAN 10 to the database server from 8:00 to 18:00 in working days.

Network diagram

Figure 1-7 Network diagram for applying an ACL to a VLAN



Configuration procedure

Define a periodic time range that is active from 8:00 to 18:00 in working days.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 working-day
```

Define an ACL to deny packets destined for the database server.

```
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 1 deny ip destination 192.168.1.2 0 time-range test
[Sysname-acl-adv-3000] quit
```

Apply ACL 3000 to VLAN 10.

```
[Sysname] packet-filter vlan 10 inbound ip-group 3000
```

Table of Contents

1 QoS Configuration

When configuring QoS, go to these sections for information you are interested in:

Overview

Introduction to QoS

Quality of Service (QoS) is a concept concerning service demand and supply. It reflects the ability to meet customer needs. Generally, QoS does not focus on grading services precisely, but on improving services under certain conditions.

In an internet, QoS refers to the ability of the network to forward packets. The evaluation on QoS of a network can be based on different aspects because the network may provide various services. Generally, QoS refers to the ability to provide improved service by solving the core issues such as delay, jitter, and packet loss ratio in the packet forwarding process.

Traditional Packet Forwarding Service

In traditional IP networks, packets are treated equally. That is, the FIFO (first in first out) policy is adopted for packet processing. Network resources required for packet forwarding is determined by the order in which packets arrive. All the packets share the resources of the network. Network resources available to the packets completely depend on the time they arrive. This service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, jitter, packet loss ratio, reliability, and so on.

The traditional Best-Effort service policy is only suitable for applications insensitive to bandwidth and delay, such as WWW, E-mail and FTP.

New Applications and New Requirements

With the expansion of computer network, more and more networks become part of the Internet. The Internet gains rapid development in terms of scale, coverage and user quantities. More and more users use the Internet as a platform for their services and for data transmission.

Besides the traditional applications such as WWW, E-mail, and FTP, new services are developed on the Internet, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD). Enterprise users expect to connect their regional branches together using VPN techniques for coping with daily business, for instance, accessing databases or manage remote equipments through Telnet.

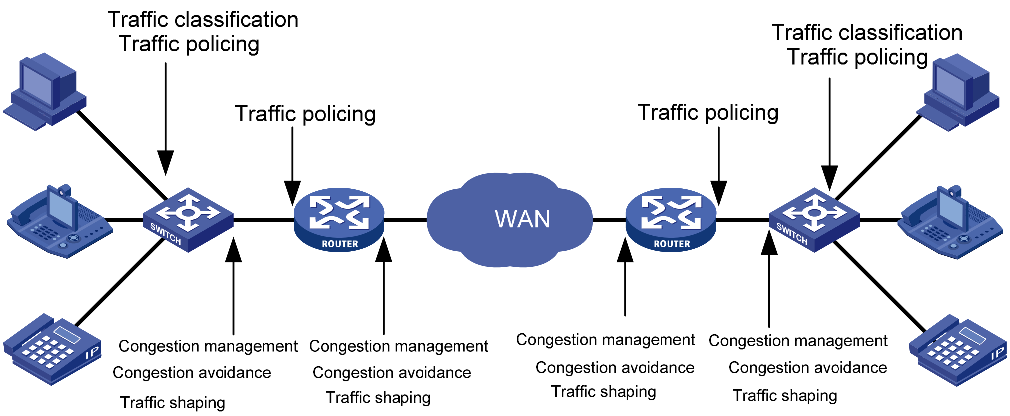
All these new applications have one thing in common, that is, they have special requirements for bandwidth, delay, and jitter. For instance, bandwidth, delay, and jitter are critical for videoconference

and VoD. As for other applications, such as transaction processing and Telnet, although bandwidth is not as critical, a too long delay may cause unexpected results. That is, they need to get serviced in time even if congestion occurs.

Newly emerging applications demand higher service performance from IP networks. In addition to simply delivering packets to their destinations, better network services are demanded, such as allocating dedicated bandwidth, reducing packet loss ratio, avoiding congestion, regulating network traffic, and setting priority of the packets. To meet those requirements, the network should be provided with better service capability.

Major Traffic Control Techniques

Figure 1-1 End-to-end QoS model



As shown in the figure above, traffic classification, traffic policing, traffic shaping, congestion management, and congestion avoidance are the foundations for a network to provide differentiated services. They are described as follow:

- Traffic classification identifies traffic based on certain matching rules. It is a prerequisite for differentiated services and is usually applied in the inbound direction of a port.
- Traffic policing confines traffic to a specific specification and is usually applied in the inbound direction of a port. You can configure restriction or penalty measures against the exceeding traffic to protect carrier benefits and network resources.
- Traffic shaping adapts output traffic rate usually to the input capability of the receiving device to avoid packet drop and port congestion. Traffic shaping is usually applied in the outbound direction of a port.
- Congestion management handles resource competition during network congestion. Generally, it adds packets to queues first, and then forwards the packets by using a scheduling algorithm. Congestion management is usually applied in the outbound direction of a port.
- Congestion avoidance monitors the use of network resources and drops packets actively when congestion reaches certain degree. It relieves network load by adjusting traffics. Congestion avoidance is usually applied in the outbound direction of a port.

Traffic classification is the basis of all the above-mentioned traffic management technologies. It identifies packets using certain rules and makes differentiated services possible. Traffic policing, traffic shaping, congestion management, and congestion avoidance are methods for implementing network traffic control and network resource management. They are occurrences of differentiated services.

QoS Supported By Switch 4500 Series

The Switch 4500 series support the QoS features listed in Table 1-1:

Table 1-1 QoS features supported by Switch 4500 series

QoS Feature	Description	Refer to …
Traffic classification	Classify incoming traffic based on ACLs. The Switch 4500 series support the following types of ACLs: • Basic ACLs • Advanced ACLs • Layer-2 ACLs • User-defined ACLs	• For information about ACLs, refer to the *ACL Operation* and *ACL Command* manuals. • For information about traffic classification, refer to Traffic Classification.
QoS action	The Switch 4500 series support performing the following QoS actions for packets matching the specified ACL: • Priority marking • Traffic policing • VLAN Mapping • Traffic mirroring	• For information about priority marking, refer to Priority Marking. • For information about traffic policing, refer to Traffic Policing. • For information about VLAN Mapping, refer to VLAN Mapping. • For information about traffic mirroring, refer to Traffic mirroring.
	You can configure the following QoS actions as required on the Switch 4500 series: • Priority trust mode • Protocol packet priority • Line rate	• For information about priority trust mode, refer to Priority Trust Mode. • For information about specifying priority for protocol packets, refer to Protocol Priority. • For information about line rate, refer toLine Rate.
Congestion avoidance	WRED	For information about congestion avoidance and WRED, refer to Congestion Avoidance.
Congestion management	The Switch 4500 series support SP, WFQ, and WRR queue scheduling algorithms and support the following five queue scheduling modes: • SP • WFQ • WRR • SP+WFQ • SP+WRR	For information about SP, WFQ, and WRR, refer to Queue Scheduling.

Introduction to QoS Functions

Traffic Classification

Traffic here refers to service traffic; that is, all the packets passing the switch.

Traffic classification means identifying packets that conform to certain characteristics according to certain rules. It is the foundation for providing differentiated services.

In traffic classification, the priority bit in the type of service (ToS) field in IP packet header can be used to identify packets of different priorities. The network administrator can also define traffic classification policies to identify packets by the combination of source address, destination address, MAC address, IP

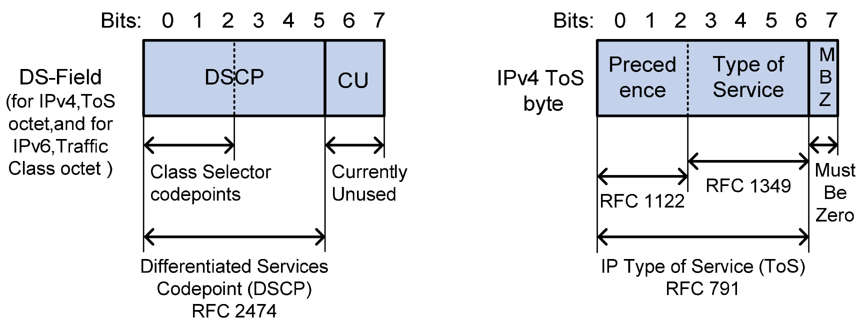
protocol or the port number of an application. Normally, traffic classification is done by checking the information carried in packet header. Packet payload is rarely adopted for traffic classification. The identifying rule is unlimited in range. It can be a quintuplet consisting of source address, source port number, protocol number, destination address, and destination port number. It can also be simply a network segment.

Priority Trust Mode

Introduction to precedence types

1) IP precedence, ToS precedence, and DSCP precedence

Figure 1-2 DS field and ToS byte



The ToS field in an IP header contains eight bits numbered 0 through 7, among which,

- The first three bits indicate IP precedence in the range 0 to 7.
- Bit 3 to bit 6 indicate ToS precedence in the range of 0 to 15.
- In RFC2474, the ToS field in IP packet header is also known as DS field. The first six bits (bit 0 through bit 5) of the DS field indicate differentiated service codepoint (DSCP) in the range of 0 to 63, and the last two bits (bit 6 and bit 7) are reserved.

Table 1-2 Description on IP Precedence

IP Precedence (decimal)	IP Precedence (binary)	Description
0	000	Routine
1	001	priority
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

In a network providing differentiated services, traffics are grouped into the following four classes, and packets are processed according to their DSCP values.

- Expedited Forwarding (EF) class: In this class, packets can be forwarded regardless of link share of other traffic. The class is suitable for preferential services with low delay, low packet loss ratio, low jitter, and assured bandwidth (such as virtual leased line);

- Assured forwarding (AF) class: This class is further divided into four subclasses (AF1/2/3/4) and a subclass is further divided into three drop priorities, so the AF service level can be segmented. The QoS rank of the AF class is lower than that of the EF class;
- Class selector (CS) class: This class comes from the IP ToS field and includes eight subclasses;
- Best Effort (BE) class: This class is a special class without any assurance in the CS class. The AF class can be degraded to the BE class if it exceeds the limit. Current IP network traffic belongs to this class by default.

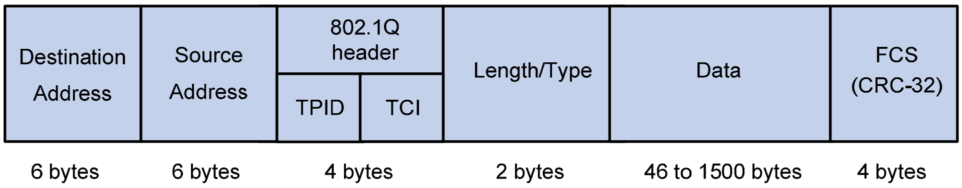
Table 1-3 Description on DSCP precedence values

DSCP value (decimal)	DSCP value (binary)	Description
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

2) 802.1p priority

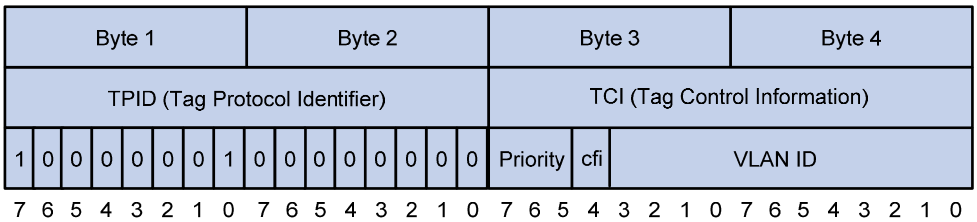
802.1p priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet header does not need analysis but QoS must be assured at Layer 2.

Figure 1-3 An Ethernet frame with an 802.1Q tag header



As shown in the figure above, the 4-byte 802.1Q tag header consists of the tag protocol identifier (TPID, two bytes in length), whose value is 0x8100, and the tag control information (TCI, two bytes in length). Figure 1-4 describes the detailed contents of an 802.1Q tag header.

Figure 1-4 802.1Q tag headers



In the figure above, the priority field (three bits in length) in TCI is 802.1p priority (also known as CoS precedence), which ranges from 0 to 7.

Table 1-4 Description on 802.1p priority

802.1p priority (decimal)	802.1p priority (binary)	Description
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

The precedence is called 802.1p priority because the related applications of this precedence are defined in detail in the 802.1p specifications.

3) Local precedence

Local precedence is a locally significant precedence that the device assigns to a packet. A local precedence value corresponds to one of the eight hardware output queues. Packets with the highest local precedence are processed preferentially. As local precedence is used only for internal queuing, a packet does not carry it after leaving the queue.

Priority trust mode

After a packet enters a switch, the switch sets the 802.1p priority and local precedence for the packet according to its own capability and the corresponding rules.

1) For a packet carrying no 802.1q tag

When a packet carrying no 802.1q tag reaches the port of a switch, the switch uses the port priority as the 802.1p precedence value of the received packet, searches for the local precedence corresponding to the port priority of the receiving port in the 802.1p-to-local precedence mapping table, and assigns the local precedence to the packet.

2) For an 802.1q tagged packet

When an 802.1q tagged packet reaches the port of a switch, you can use the **priority trust** on the receiving port to configure the port to trust packet priority or use the **priority** command on the receiving port to configure the port to trust port priority. By default, port priority is trusted and the priority of a port is 0.

- Trusting port priority

In this mode, the switch replaces the 802.1p priority of the received packet with the port priority, searches for the local precedence corresponding to the port priority of the receiving port in the 802.1p-to-local precedence mapping table, and assigns the local precedence to the packet.

- Trusting packet priority

In this mode, the switch searches for the local precedence corresponding to the 802.1p priority of the packet in the 802.1p-to-local precedence mapping table and assigns the local precedence to the packet.

Table 1-5 shows the default 802.1p priority-to-local precedence mapping table. You can modify the default mapping tables at the CLI. For detailed configuration procedure, refer to Configuring the Mapping between 802.1p Priority and Local Precedence.

Table 1-5 802.1p priority-to-local precedence mapping table

802.1p priority	Local precedence
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Protocol Priority

Protocol packets generated by a switch carry their own priority. You can set a new IP precedence or DSCP precedence for the specific type of protocol packets to implement QoS.

Priority Marking

The priority marking function is to reassign priority for the traffic matching an ACL referenced for traffic classification.

- If 802.1p priority marking is configured, the traffic will be mapped to the local precedence corresponding to the re-marked 802.1p priority and assigned to the output queue corresponding to the local precedence.
- If local precedence marking is configured, the traffic will be assigned to the output queue corresponding to the re-marked local precedence.
- If IP precedence or DSCP marking is configured, the traffic will be marked with new IP precedence or DSCP precedence.

Traffic Policing

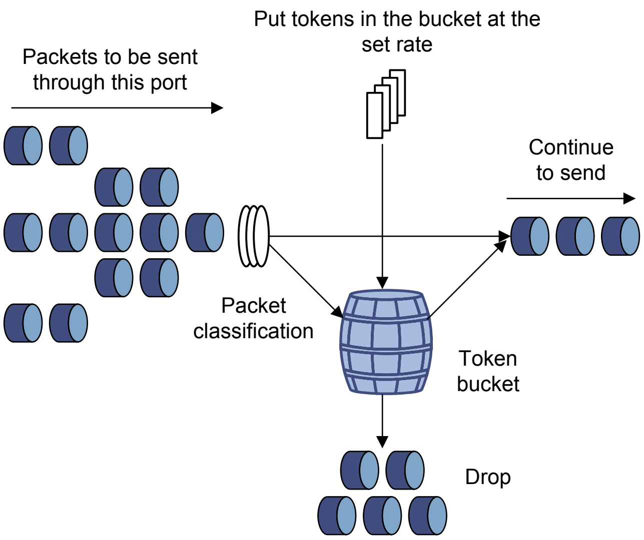
The network will be made more congested by plenty of continuous burst packets if the traffic of each user is not limited. The traffic of each user must be limited in order to make better use of the limited network resources and provide better service for more users. For example, traffic can be limited to get only its committed resources during a time period to avoid network congestion caused by excessive bursts.

Traffic policing is a kind of traffic control policy used to limit the traffic and the resource occupied by supervising the traffic. The regulation policy is implemented according to the evaluation result on the premise of knowing whether the traffic exceeds the specification when traffic policing is performed. Normally, token bucket is used for traffic evaluation.

Token bucket

The token bucket can be considered as a container with a certain capacity to hold tokens. The system puts tokens into the bucket at the set rate. When the token bucket is full, the extra tokens will overflow and the number of tokens in the bucket stops increasing.

Figure 1-5 Evaluate the traffic with the token bucket



Evaluating the traffic with the token bucket

When token bucket is used for traffic evaluation, the number of the tokens in the token bucket determines the amount of the packets that can be forwarded. If the number of tokens in the bucket is

enough to forward the packets, the traffic is conforming to the specification; otherwise, the traffic is nonconforming or excess.

Parameters concerning token bucket include:

- Average rate: The rate at which tokens are put into the bucket, namely, the permitted average rate of the traffic. It is generally set to committed information rate (CIR).
- Burst size: The capacity of the token bucket, namely, the maximum traffic size that is permitted in each burst. It is generally set to committed burst size (CBS). The set burst size must be greater than the maximum packet length.

One evaluation is performed on each arriving packet. In each evaluation, if the number of tokens in the bucket is enough, the traffic is conforming to the specification and you must take away some tokens whose number is corresponding to the packet forwarding authority; if the number of tokens in the bucket is not enough, it means that too many tokens have been used and the traffic is excess.

Traffic policing

The typical application of traffic policing is to supervise specific traffic into the network and limit it to a reasonable range, or to "discipline" the extra traffic. In this way, the network resources and the interests of the operators are protected. For example, you can limit HTTP packets to be within 50% of the network bandwidth. If the traffic of a certain connection is excess, traffic policing can choose to drop the packets or to reset the priority of the packets.

Traffic policing is widely used in policing the traffic into the network of internet service providers (ISPs). Traffic policing can identify the policed traffic and perform pre-defined policing actions based on different evaluation results. These actions include:

- Drop. Drop the packet whose evaluation result is “nonconforming”.
- Modify the DSCP precedence and forward. Modify the DSCP precedence of the packets whose evaluation result is “nonconforming” and then forward them.

Line Rate

Line rate refers to limiting the total rate of inbound or outbound packets on a port.

Line rate can be implemented through token buckets. That is, if you perform line rate configuration for a port, the token bucket determines the way to process the packets to be sent by this port or packets reaching the port. Packets can be sent or received if there are enough tokens in the token bucket; otherwise, they will be dropped.

Compared to traffic policing, line rate applies to all the packets passing a port. It is a simpler solution if you want to limit the rate of all the packets passing a port.

VLAN Mapping

VLAN mapping identifies traffics using ACLs and maps the VLAN tags carrier in matched packets to specific VLAN tags. By employing VLAN mapping on a switch connecting user networks to the carrier network, you can map the VLAN tags of specific user network packets to those of specific VLANs in the carrier network, thus meeting the requirements of the carrier network.

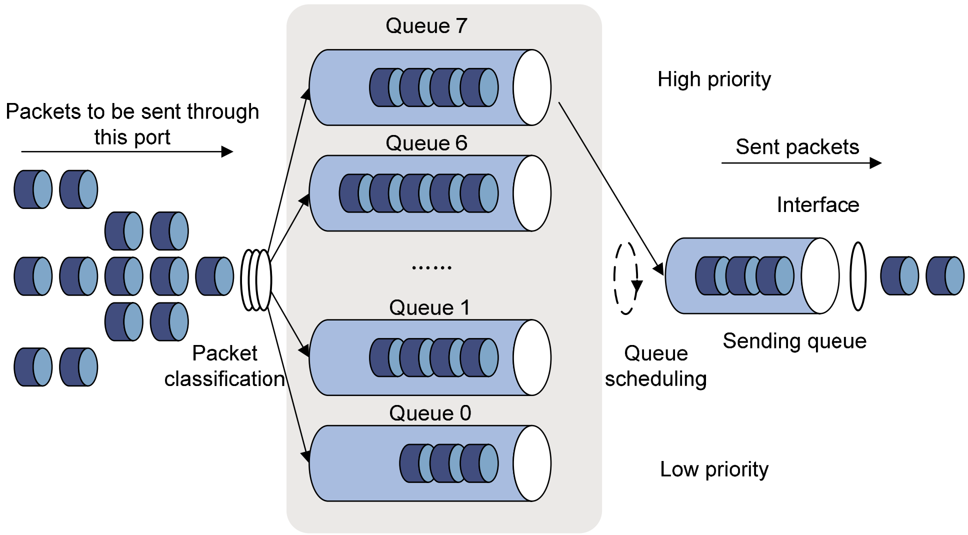
Queue Scheduling

When the network is congested, the problem that many packets compete for resources must be solved, usually through queue scheduling.

The Switch 4500 series support three queue scheduling algorithms: Strict Priority (SP) queuing, Weighted Fair Queuing (WFQ), and Weighted Round Robin (WRR) queuing.

1) SP queuing

Figure 1-6 Diagram for SP queuing



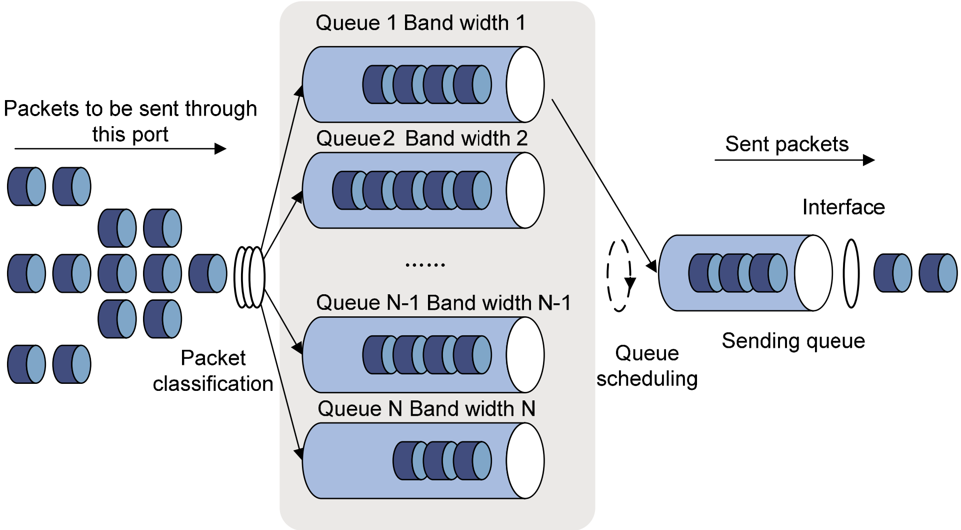
SP queue-scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay. Assume that there are eight output queues on the port and the preferential queue classifies the eight output queues on the port into eight classes, which are queue7, queue6, queue5, queue4, queue3, queue2, queue1, and queue0. Their priorities decrease in order.

In queue scheduling, SP sends packets in the queue with higher priority strictly following the priority order from high to low. When the queue with higher priority is empty, packets in the queue with lower priority are sent. You can put critical service packets into the queues with higher priority and put non-critical service (such as e-mail) packets into the queues with lower priority. In this case, critical service packets are sent preferentially and non-critical service packets are sent when critical service groups are not sent.

The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be "starved" because they are not served.

2) WFQ queuing

Figure 1-7 Diagram for WFQ queuing



Before WFQ is introduced, you must understand fair queuing (FQ) first. FQ is designed for the purpose of sharing network resources fairly and optimizing the delays and delay jitters of all the flows. It takes the interests of all parties into account, such as:

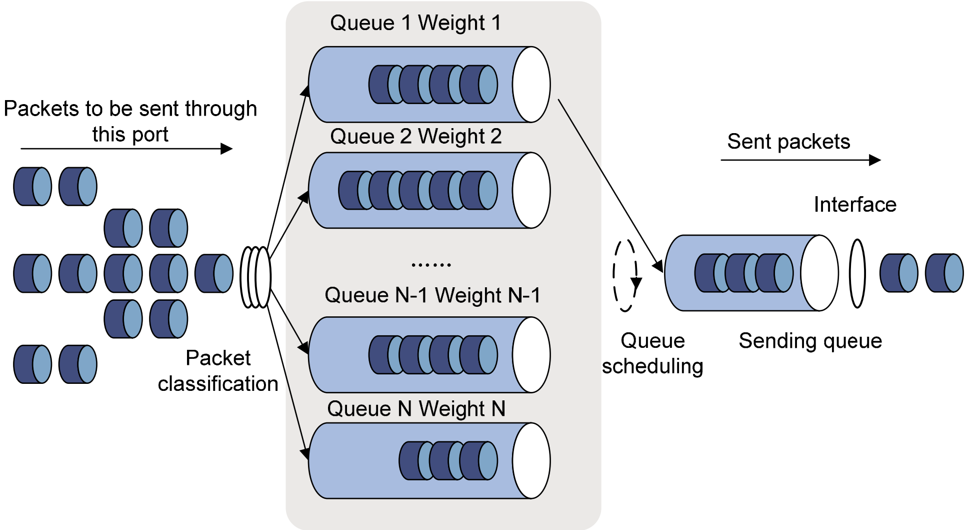
- Different queues are scheduled fairly, so the delay of each flow is balanced globally.
- Both short and long packets are scheduled fairly. When there are multiple long packets and short packets to be sent among different queues, the short packets must be scheduled preferentially, so that the delay jitters of packets of each flow is reduced globally.

Compared with FQ, WFQ takes the priority into account when calculating the scheduling sequence of packets. Statistically speaking, WFQ assigns more scheduling chances to high priority packets than those to low priority packets. WFQ can classify the traffic automatically according to the session information of traffic including the protocol types, source and destination TCP or UDP port numbers, source and destination IP addresses, and priority values in the ToS field. WFQ also provide as many queues as possible to accommodate each flow evenly. Thus, the delay of each flow is balanced globally. When the packets dequeue, WFQ assigns the bandwidth to each flow on the egress according to the traffic precedence or DSCP precedence. The lower the traffic precedence is, the less bandwidth the traffic gets. The higher the traffic precedence is, the more bandwidth the traffic gets. Finally, each queue is polled and the corresponding number of packets is taken out to be sent according to the proportion of bandwidth.

You can use the WFQ algorithm to assign bandwidth to the output queues of a port, and then decide which queue a traffic flows into according to the mapping between the COS value of the traffic and the queue, and also deicide how much bandwidth is to be assigned to each traffic.

3) WRR queuing

Figure 1-8 Diagram for WRR queuing



WRR queue-scheduling algorithm schedules all the queues in turn and every queue can be assured of a certain service time.

In a typical 3Com switch there are eight output queues on each port. WRR configures a weight value for each queue, for example: w7, w6, w5, w4, w3, w2, w1, and w0 respectively for queue 7 through queue 0. A weight value indicates the proportion of resources available for a queue. On a 100-Mbps port, configure the weight value of WRR queue-scheduling algorithm to 5, 5, 3, 3, 1, 1, 1, and 1 (corresponding to w7, w6, w5, w4, w3, w2, w1, and w0 in order). In this way, the queue with the lowest priority can get 5 Mbps (100 Mbps × 1/(5+5+3+3+1+1+1+1)) bandwidth at least, and the disadvantage of SP queue-scheduling that the packets in queues with lower priority may not get service for a long time is avoided. Another advantage of WRR queue is that: though the queues are scheduled in order, the service time for each queue is not fixed; that is to say, if a queue is empty, the next queue will be scheduled. In this way, the bandwidth resources are made full use.

Congestion Avoidance

Congestion may cause network resource unavailable and thus need to be prevented. As a type of flow control mechanism, congestion avoidance aims to relieve network load through traffic adjusting. With congestion avoidance configuration performed, packets are dropped in advance when the utilization of certain network resources (such as output queues or buffer created in the memory) reaches certain degree.

Traditional packet dropping policy

Tail drop is adopted in traditional packet drop policies. It drops all the newly arrived packets when the current queue length reaches a specific value.

Such a policy will result in global TCP connection synchronization. If a queue drops packets of multiple TCP connections simultaneously, the TCP connections will turn to the state of congestion avoidance and slow startup for the traffics to be regulated. The traffic peak will then occur in a certain future time. Consequently, the network traffic jitters all the time.

WRED

You can use weighted random early detection (WRED) to avoid global TCP session synchronization.

In WRED algorithm, an upper limit and a lower limit are set for each queue, and the packets in a queue are processed as follows.

- When the current queue length is smaller than the lower limit, no packet is dropped;
- When the queue length exceeds the upper limit, all the newly received packets are dropped;
- When the queue length is between the lower limit and the upper limit, the newly received packets are dropped at random. The longer the queue, the more likely the newly received packets may be dropped. However, a maximum drop probability exists.

In WRED, random numbers are generated to determine the packets to be dropped. As the dropping policy is determined by IP precedence, packets with lower precedence are more likely to be dropped.

WRED prevents global TCP session synchronization. It enables other TCP sessions to be free of a TCP session slowed down because of its packets being dropped. In this way, TCP sessions can operate in different rates in any case and the link bandwidth can be fully utilized.

Traffic mirroring

Traffic mirroring identifies traffic using ACLs and duplicates the matched packets to the destination mirroring port or CPU depending on your configuration. For information about port mirroring, refer to the Mirroring module of this manual.

QoS Configuration

Complete the following tasks to configure QoS:

Task	Remarks
Configuring Priority Trust Mode	Optional
Configuring the Mapping between 802.1p Priority and Local Precedence	Optional
Setting the Priority of Protocol Packets	Optional
Marking Packet Priority	Optional
Configuring Traffic Policing	Optional
Configuring Line Rate	Optional
Configuring VLAN Mapping	Optional
Configuring Queue Scheduling	Optional
Configuring WRED	Optional
Configuring Traffic Mirroring	Optional

Configuring Priority Trust Mode

Refer to section Priority Trust Mode for introduction to priority trust mode.

Configuration prerequisites

- The priority trust mode to be adopted has been determined.
- The port where priority trust mode is to be configured has been determined.
- The port priority value has been determined.

Configuration procedure

Follow these steps to configure to trust port priority:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure to trust port priority and configure the port priority	**priority** *priority-level*	Optional By default, the switch trusts port priority and the priority of a port is 0.

Follow these steps to configure to trust packet priority:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure to trust packet priority	**priority trust**	Required By default, the switch trusts port priority.

Configuration example

- Configure to trust port priority on Ethernet 1/0/1 and set the priority of Ethernet 1/0/1 to 7.

Configuration procedure:

```
<Sysname> system-view
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] priority 7
```

- Configure to trust packet priority on Ethernet 1/0/2.

Configuration procedure:

```
<Sysname> system-view
[Sysname] interface Ethernet1/0/2
[Sysname-Ethernet1/0/2] priority trust
```

Configuring the Mapping between 802.1p Priority and Local Precedence

When the default mapping between 802.1p priority and local precedence cannot satisfy your requirements, you can modify the mapping at the CLI, thus modifying the mapping between 802.1p priority and the output queues and assigning packets with different priorities to the corresponding output queues.

Note that, this is a global setting, not a per port setting. This is only recommended for advanced network environments.

Configuration prerequisites

The mapping between 802.1p priority and local precedence has been determined.

Configuration procedure

Follow these steps to configure the mapping between 802.1p priority and local precedence:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the mapping between 802.1p priority and local precedence	**qos cos-local-precedence-map** *cos0-map-local-prec cos1-map-local-prec cos2-map-local-prec cos3-map-local-prec cos4-map-local-prec cos5-map-local-prec cos6-map-local-prec cos7-map-local-prec*	Required

Configuration example

- Configure the following mapping between 802.1p priority and local precedence: 0 to 2, 1 to 3, 2 to 4, 3 to 1, 4 to 7, 5 to 0, 6 to 5, and 7 to 6.
- Display the configuration.

Configuration procedure:

```
<Sysname> system-view
[Sysname] qos cos-local-precedence-map 2 3 4 1 7 0 5 6
[Sysname] display qos cos-local-precedence-map
 cos-local-precedence-map:
           cos(802.1p) :      0     1     2     3     4     5     6     7
--------------------------------------------------------------------------
local precedence(queue) :     2     3     4     1     7     0     5     6
```

Setting the Priority of Protocol Packets

Refer to section Protocol Priority for information about priority of protocol packets.

Configuration prerequisites

- The protocol type has been determined.
- The priority type (IP or DSCP) and priority value have been determined.

Configuration procedure

Follow these steps to set the priority for specific protocol packets:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the priority for specific protocol packets	**protocol-priority protocol-type** *protocol-type* { **ip-precedence** *ip-precedence* | **dscp** *dscp-value* }	Required You can modify the IP precedence or DSCP precedence of the corresponding protocol packets.

Note

On Switch 4500, you can set the priority for protocol packets of Telnet, SNMP, and ICMP.

Configuration example

- Set the IP precedence of ICMP packets to 3.
- Display the configuration.

Configuration procedure:

```
<Sysname> system-view
[Sysname] protocol-priority protocol-type icmp ip-precedence 3
[Sysname] display protocol-priority
Protocol: icmp
  IP-Precedence: flash(3)
```

Marking Packet Priority

Refer to section Priority Marking for information about marking packet priority.

Marking packet priority can be implemented in the following two ways:

- Through traffic policing

When configuring traffic policing, you can define the action of marking the DSCP precedence for packets exceeding the traffic specification. Refer to section Configuring Traffic Policing.

- Through the **traffic-priority** command

You can use the **traffic priority** command to mark the IP precedence, 802.1p priority, DSCP precedence, and local precedence of the packets.

Configuration prerequisites

The following items are defined or determined before the configuration:

- The ACL rules used for traffic classification have been specified. Refer to the ACL module of this manual for related information.
- The type and value of the precedence to be marked for the packets matching the ACL rules have been determined.
- The port or VLAN on which the configuration is to be performed has been determined.

Configuration procedure

Follow these steps to configure priority marking on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Mark the priorities for packets matching specific ACL rules	**traffic-priority** { **inbound** | **outbound** } *acl-rule* { { **dscp** *dscp-value* | **ip-precedence** { *pre-value* | **from-cos** } } | **cos** { *pre-value* | **from-ipprec** } | **local-precedence** *pre-value* }*	Required Refer to the command manual for information about the *acl-rule* argument.

Follow these steps to configure priority marking on a VLAN:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Mark the priorities for the packets belonging to a VLAN and matching specific ACL rules	**traffic-priority vlan** *vlan-id* { **inbound** | **outbound** } *acl-rule* { { **dscp** *dscp-value* | **ip-precedence** { *pre-value* | **from-cos** } } | **cos** { *pre-value* | **from-ipprec** } | **local-precedence** *pre-value* }*	Required Refer to the command manual for information about the *acl-rule* argument.

Configuration example

- Ethernet 1/0/1 belongs to VLAN 2 and is connected to the 10.1.1.1/24 network segment.
- Mark the DSCP precedence as 56 for the packets from the 10.1.1.1/24 network segment.

1) Method I

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] traffic-priority inbound ip-group 2000 dscp 56
```

2) Method II

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] traffic-priority vlan 2 inbound ip-group 2000 dscp 56
```

Configuring Traffic Policing

Refer to section Traffic Policing for information about traffic policing.

Configuration prerequisites

- The ACL rules used for traffic classification have been defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The rate limit for traffic policing, and the actions for the packets exceeding the rate limit have been determined.
- The ports that need this configuration have been determined.

Configuration procedure

Follow these steps to configure traffic policing:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

To do…	Use the command…	Remarks
Configure traffic policing	**traffic-limit inbound** *acl-rule* [**union-effect**] *target-rate* [**burst-bucket** *burst-bucket-size*] [**exceed** *action*]	Required Specify a committed information rate (CIR) for the *target-rate* argument, and specify a committed bust size (CBS) for the *burst-bucket-size* argument. By default, traffic policing is disabled.

Note

The granularity of traffic policing is 64 Kbps. If the number you input is in the range of N*64 to (N+1)*64 (N is a natural number), it will be rounded off to (N+1)*64.

Configuration example

- Ethernet 1/0/1 of the switch is connected to the 10.1.1.0/24 network segment
- Perform traffic policing on the packets from the 10.1.1.0/24 network segment, setting the rate to 128 kbps
- Mark the DSCP precedence as 56 for the inbound packets exceeding the rate limit.

Configuration procedure:

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] traffic-limit inbound ip-group 2000 128 exceed remark-dscp 56
```

Configuring Line Rate

Refer to section Line Rate for information about line rate.

Configuration prerequisites

- The port on which line rate configuration is to be performed has been determined.
- The target rate and the direction of rate limiting (inbound or outbound) have been determined.

Configuration procedure

Follow these steps to configure line rate:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—

To do…	Use the command…	Remarks
Configure line rate	**line-rate** { **inbound** | **outbound** } *target-rate* [**burst-bucket** *burst-bucket-size*]	Required Specify a committed information rate (CIR) for the *target-rate* argument, and specify a committed bust size (CBS) for the *burst-bucket-size* argument. By default, line rate is disabled.

Configuration example

- Configure line rate for outbound packets on Ethernet 1/0/1.
- The rate limit is 1,024 Kbps

Configuration procedure:

```
<Sysname> system-view
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] line-rate outbound 1024
```

Configuring VLAN Mapping

Refer to section VLAN Mapping for information about VLAN mapping.

Configuration prerequisites

- The ACL rules used for traffic classification have been defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The ports on which the configuration is to be performed have been determined.
- The VLAN ID to be set for the packets has been determined.

Configuration procedure

Follow these steps to configure VLAN mapping:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure VLAN mapping	**traffic-remark-vlanid inbound** *acl-rule* **remark-vlan** *remark-vlanid*	Required By default, VLAN mapping is not configured.

Configuring Queue Scheduling

Refer to section Queue Scheduling for information about queue scheduling.

Configuration prerequisites

The algorithm for queue scheduling to be used and the related parameters have been determined.

Configuration procedure

Follow these steps to configure queue scheduling in system view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure queue scheduling	**queue-scheduler** { **strict-priority** | **wfq** *queue0-width queue1-width queue2-width queue3-width queue4-width queue5-width queue6-width queue7-width* | **wrr** *queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight* }	Required By default, the queue scheduling algorithm adopted on all the ports is WRR. The default weights of the eight output queues of a port are 1, 2, 3, 4, 5, 9, 13, and 15 (in the order queue 0 through queue 7).

Follow these steps to configure queue scheduling in Ethernet port view:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure queue scheduling	**queue-scheduler** { **wfq** *queue0-width queue1-width queue2-width queue3-width queue4-width queue5-width queue6-width queue7-width* | **wrr** *queue0-weight queue1-weight queue2-weight queue3-weight queue4-weight queue5-weight queue6-weight queue7-weight* }	Required By default, the queue scheduling algorithm adopted on all the ports is WRR. The default weights of the eight output queues of a port are 1, 2, 3, 4, 5, 9, 13, and 15 (in the order queue 0 through queue 7).

A port of a Switch 4500 supports eight output queues. These queue scheduling algorithms are available: SP, WRR, and WFQ. With WRR (or WFQ) adopted, if you set the weight or the bandwidth of one or multiple queues to 0, the switch will add the queue or these queues to the SP group, where SP is adopted. For other queues, WRR (or WFQ) still applies. In this case, both SP and WRR (or WFQ) are adopted.

In cases where both SP and WRR (or WFQ) queue scheduling algorithms are adopted, the queues in the SP group take precedence over other queues. For example, if queue 0, queue 1, queue 2, and queue 3 are in the SP group, queue 4, queue 5, queue 6, and queue 7 are scheduled using WRR (or WFQ), the switch will schedule the queues in the SP group preferentially by using the SP algorithm. Then queues outside the SP group are scheduled by using WRR (or WFQ) algorithm only when all the queues in the SP group are empty.

Note

- The queue scheduling algorithm specified by using the **queue-scheduler** command in system view takes effect on all the ports. The queue scheduling algorithm configured in port view must be the same as that configured in system view. Otherwise, the system prompts configuration errors.
- If the weight (or bandwidth value) specified in system view for a queue of WRR queuing or WFQ queuing cannot meet the requirement of a port, you can modify the weight (or bandwidth value) for this port in the corresponding Ethernet port view. The new weight (or bandwidth value) takes effect only on the port.
- If the weight (or bandwidth value) specified in system view for a queue of SP-WRR queuing or SP-WFQ queuing in the command cannot meet the requirement of a port, you can modify the weight (or bandwidth value) for this port in the corresponding Ethernet port view. The new weight (or bandwidth value) takes effect only on the port.
- The **display queue-scheduler** command cannot display the queue weight (or bandwidth value) specified in Ethernet port view.

Configuration example

- Adopts WRR for queue scheduling, setting the weights of the output queues to 2, 2, 3, 3, 4, 4, 5, and 5 (in the order queue 0 through queue 7).
- Verify the configuration.

Configuration procedure:

```
<Sysname> system-view
[Sysname] queue-scheduler wrr 2 2 3 3 4 4 5 5
[Sysname] display queue-scheduler
 Queue scheduling mode: weighted round robin
 weight of queue 0: 2
 weight of queue 1: 2
 weight of queue 2: 3
 weight of queue 3: 3
 weight of queue 4: 4
 weight of queue 5: 4
 weight of queue 6: 5
 weight of queue 7: 5
```

Configuring WRED

Refer to section Congestion Avoidance for information about WRED.

Configuration prerequisites

- The indexes of queues to be dropped at random, the queue length that starts the drop action, and the drop probability have been determined.
- The ports that need this configuration have been determined.

Configuration procedure

Follow these steps to configure WRED:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure WRED	**wred** *queue-index qstart probability*	Required By default, WRED is not configured.

Configuration example

Configure WRED for queue 2 of Ethernet 1/0/1 to drop the packets in queue 2 randomly when the number of packets in queue 2 exceeds 64, setting the dropping probability being 20%.

Configuration procedure:

```
<Sysname> system-view
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] wred 2 64 20
```

Configuring Traffic Mirroring

Refer to section Traffic mirroring for information about traffic mirroring.

Configuration prerequisites

- The ACL rules for traffic classification have been defined. Refer to the ACL module of this manual for information about defining ACL rules.
- The source mirroring ports and mirroring direction have been determined.
- The destination mirroring port has been determined.

Configuration procedure

Follow these steps to configure traffic mirroring:

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="2">Enter Ethernet port view</td><td>interface interface-type interface-number</td><td>—</td></tr>
<tr><td colspan="2">Configure the current port as a source mirroring port</td><td>mirrored-to { inbound | outbound } acl-rule { monitor-interface | cpu }</td><td>Required
Omit the following steps if you redirect traffic to the CPU.
Proceed to the following steps if you redirect traffic to a port.</td></tr>
<tr><td colspan="2">Quit to system view</td><td>quit</td><td>—</td></tr>
<tr><td rowspan="3">Configure the specified port as the destination mirroring port</td><td>In system view</td><td>mirroring-group group-id monitor-port monitor-port-id</td><td rowspan="3">Required
Use either approach.</td></tr>
<tr><td rowspan="2">In Ethernet port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>monitor-port</td></tr>
</table>

Note

For information about the **mirroring-group monitor-port** command and the **monitor-port** command, refer to the part talking about mirroring.

Configuration example

Network requirements:

- Ethernet 1/0/1 is connected to the 10.1.1.0/24 network segment.
- Duplicate the packets from network segment 10.1.1.0/24 to the destination mirroring port Ethernet 1/0/4.

Configuration procedure:

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] interface Ethernet1/0/4
[Sysname-Ethernet1/0/4] monitor-port
[Sysname-Ethernet1/0/4] quit
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] mirrored-to inbound ip-group 2000 monitor-interface
```

Displaying and Maintaining QoS

To do…	Use the command…	Remarks
Display the mapping between 802.1p priority and local precedence	**display qos cos-local-precedence-map**	Available in any view
Display the priority marking configuration	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-priority**	
Display the protocol packet priority configuration	**display protocol-priority**	
Display line rate configuration	**display qos-interface** { *interface-type interface-number* | *unit-id* } **line-rate**	
Display traffic policing configuration	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-limit**	
Display VLAN mapping configuration	**display qos-interface** { *interface-type interface-number* | *unit-id* } **traffic-remark-vlanid**	
Display queue scheduling configuration	**display queue-scheduler**	
Display traffic mirroring configuration	**display qos-interface** { *interface-type interface-number* | *unit-id* } **mirrored-to**	
Display all the QoS configuration	**display qos-interface** { *interface-type interface-number* | *unit-id* } **all**	

QoS Configuration Examples

Configuration Example of Traffic policing and Line Rate

Network requirement

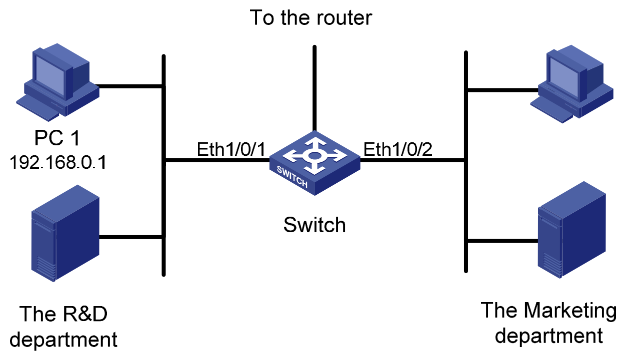
An enterprise network connects all the departments through an Ethernet switch. PC 1, with the IP address 192.168.0.1 belongs to the R&D department and is connected to Ethernet 1/0/1 of the switch. The marketing department is connected to Ethernet 1/0/2 of the switch.

Configure traffic policing and line rate to satisfy the following requirements:

- Set the maximum rate of outbound packets sourced from the marketing department to 64 kbps. Drop the packets exceeding the rate limit.
- Set the maximum rate of outbound IP packets sent by PC 1 in the R&D department to 640 kbps. Drop the packets exceeding the rate limit.

Network diagram

Figure 1-9 Network diagram for traffic policing and rate limiting configuration



Configuration procedure

1) Define an ACL for traffic classification.

Create ACL 2000 and enter basic ACL view.

```
<Sysname> system-view
[Sysname] acl number 2000
```

Define a rule for the packets with 192.168.0.1 as the source IP address.

```
[Sysname-acl-basic-2000] rule permit source 192.168.0.1 0
[Sysname-acl-basic-2000] quit
```

2) Configure traffic policing and rate limiting

Set the maximum rate of outbound packets sourced from the marketing department to 64 kbps.

```
[Sysname] interface Ethernet1/0/2
[Sysname-Ethernet1/0/2] line-rate inbound 64
[Sysname-Ethernet1/0/2] quit
```

Set the maximum rate of outbound IP packets sent by PC 1 in the R&D department to 640 kbps.

```
[Sysname] interface Ethernet1/0/1
[Sysname-Ethernet1/0/1] traffic-limit inbound ip-group 2000 640 exceed drop
```

Configuration Example of Priority Marking and Queue Scheduling

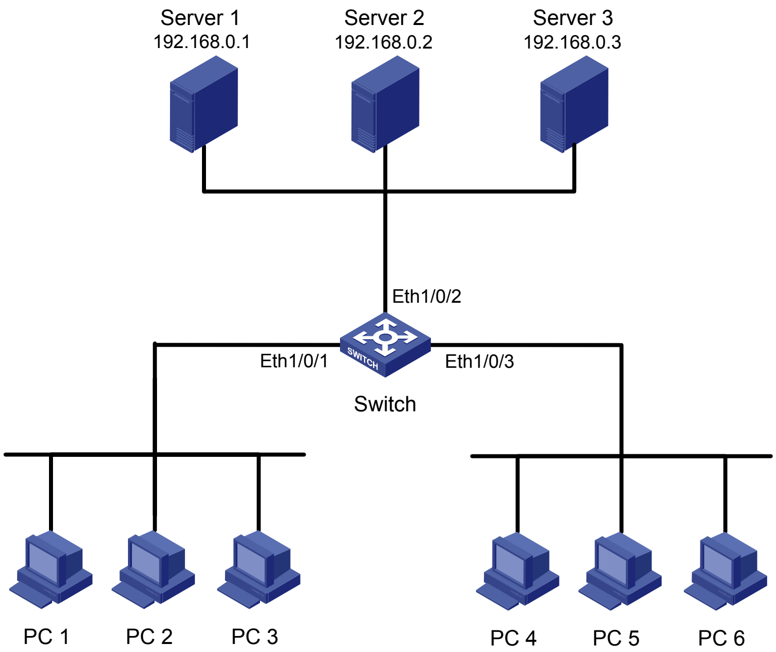
Network requirements

As shown in Figure 1-10, an enterprise network connects all the departments through an Ethernet switch. Clients PC 1 through PC 3 are connected to Ethernet 1/0/1 of the switch; clients PC 4 through PC 6 are connected to Ethernet 1/0/3 of the switch. Server 1 (the database server), Server 2 (the mail server), and Server 3 (the file server) are connected to Ethernet 1/0/2 of the switch.

Configure priority marking and queue scheduling on the switch to mark traffic flows accessing Server 1, Server 2, and Server 3 with different priorities respectively and assign the three traffic flows to different queues for scheduling.

Network diagram

Figure 1-10 Network diagram for priority marking and queue scheduling configuration



Configuration procedure

1) Define an ACL for traffic classification

Create ACL 3000 and enter advanced ACL view.

```
<Sysname> system-view
[Sysname] acl number 3000
```

Define ACL rules for identifying packets based on destination IP addresses.

```
[Sysname-acl-adv-3000] rule 0 permit ip destination 192.168.0.1 0
[Sysname-acl-adv-3000] rule 1 permit ip destination 192.168.0.2 0
[Sysname-acl-adv-3000] rule 2 permit ip destination 192.168.0.3 0
[Sysname-acl-adv-3000] quit
```

2) Configure priority marking

Mark priority for packets received through Ethernet 1/0/2 and matching ACL 3000.

```
[Sysname] interface Ethernet1/0/2
[Sysname-Ethernet1/0/2] traffic-priority inbound ip-group 3000 rule 0 local-precedence 4
```

```
[Sysname-Ethernet1/0/2] traffic-priority inbound ip-group 3000 rule 1 local-precedence 3
[Sysname-Ethernet1/0/2] traffic-priority inbound ip-group 3000 rule 2 local-precedence 2
[Sysname-Ethernet1/0/2] quit
```

3) Configure queue scheduling

Apply SP queue scheduling algorithm.

```
[Sysname] queue-scheduler strict-priority
```

VLAN Mapping Configuration Example

Network requirements

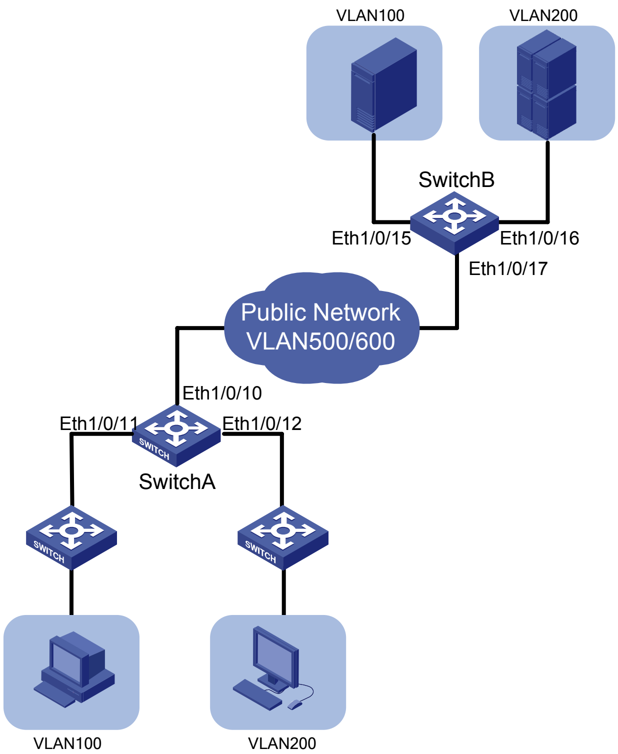
Two customer networks are connected to the public network through Switch A and Switch B. Configure the VLAN mapping function on the switches to enable the hosts on the two customer networks to communicate through public network VLANs.

- Switch A provides network access for terminal devices in VLAN 100 and VLAN 200 through Ethernet 1/0/11 and Ethernet 1/0/12. On the other side of the public network, Switch B provides network access for servers in VLAN 100 and VLAN 200 through Ethernet 1/0/15 and Ethernet 1/0/16.
- Switch A provides access to the public network through Ethernet 1/0/10 and Switch B provides access to the public network through Ethernet 1/0/17.

Configure the switches to have packets of VLAN 100 and packets of VLAN 200 transmitted in VLAN 500 and VLAN 600 across the public network.

Network diagram

Figure 1-11 Network diagram for VLAN mapping configuration



Configuration procedure

Create customer VLANs VLAN 100 and VLAN 200 and service VLANs VLAN 500 and VLAN 600 on Switch A.

```
<SwitchA> system-view
[SwitchA] vlan 100
[SwitchA-vlan100] quit
[SwitchA] vlan 200
[SwitchA-vlan200] quit
[SwitchA] vlan 500
[SwitchA-vlan500] quit
[SwitchA] vlan 600
[SwitchA-vlan600] quit
```

Configure Ethernet 1/0/11 of Switch A as a trunk port and configure its default VLAN as VLAN 100. Assign Ethernet 1/0/11 to VLAN 100 and VLAN 500. Configure Ethernet 1/0/12 in the same way.

```
[SwitchA] interface Ethernet 1/0/11
[SwitchA-Ethernet1/0/11] port link-type trunk
[SwitchA-Ethernet1/0/11] port trunk pvid vlan 100
[SwitchA-Ethernet1/0/11] port trunk permit vlan 100 500
[SwitchA-Ethernet1/0/11] quit
[SwitchA] interface Ethernet 1/0/12
[SwitchA-Ethernet1/0/12] port link-type trunk
[SwitchA-Ethernet1/0/12] port trunk pvid vlan 200
[SwitchA-Ethernet1/0/12] port trunk permit vlan 200 600
[SwitchA-Ethernet1/0/12] quit
```

Configure Ethernet 1/0/10 of Switch A as a trunk port, and assign it to VLAN 100, VLAN 200, VLAN 500, and VLAN 600.

```
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] port link-type trunk
[SwitchA-Ethernet1/0/10] port trunk permit vlan 100 200 500 600
[SwitchA-Ethernet1/0/10] quit
```

Configure Layer-2 ACLs on Switch A. Configure ACL 4000 to permit packets from VLAN 100, ACL 4001 to permit packets from VLAN 200, ACL 4002 to permit packets from VLAN 500, and ACL 4003 to permit packets from VLAN 600.

```
[SwitchA] acl number 4000
[SwitchA-acl-ethernetframe-4000] rule permit source 100
[SwitchA] quit
[SwitchA] acl number 4001
[SwitchA-acl-ethernetframe-4001] rule permit source 200
[SwitchA] quit
[SwitchA] acl number 4002
[SwitchA-acl-ethernetframe-4002] rule permit source 500
[SwitchA] quit
[SwitchA] acl number 4003
[SwitchA-acl-ethernetframe-4003] rule permit source 600
[SwitchA] quit
```

Configure VLAN mapping on Ethernet 1/0/11 to replace VLAN tag 100 with VLAN tag 500.

```
[SwitchA] interface Ethernet 1/0/11
[SwitchA-Ethernet1/0/11] traffic-remark-vlanid inbound link-group 4000 remark-vlan 500
[SwitchA-Ethernet1/0/11] quit
```

Configure VLAN mapping on Ethernet 1/0/12 to replace VLAN tag 200 with VLAN tag 600.

```
[SwitchA] interface Ethernet 1/0/12
[SwitchA-Ethernet1/0/12] traffic-remark-vlanid inbound link-group 4001 remark-vlan 600
[SwitchA-Ethernet1/0/12] quit
```

Configure VLAN mapping on Ethernet 1/0/10 to replace VLAN tag 500 with VLAN tag 100 and replace VLAN tag 600 with VLAN tag 200.

```
[SwitchA] interface Ethernet 1/0/10
[SwitchA-Ethernet1/0/10] traffic-remark-vlanid inbound link-group 4002 remark-vlan 100
[SwitchA-Ethernet1/0/10] traffic-remark-vlanid inbound link-group 4003 remark-vlan 200
[SwitchA-Ethernet1/0/10] quit
```

Define the same VLAN mapping rules on Switch B. The detailed configuration procedure is similar to that of Switch A and thus is omitted here.

Table of Contents

1 Mirroring Configuration

When configuring mirroring, go to these sections for information you are interested in:

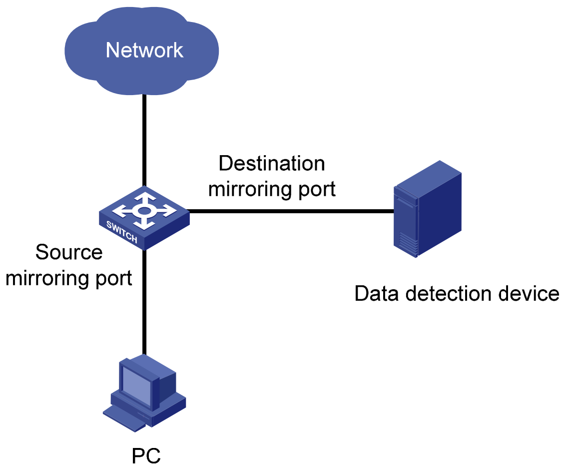
- Mirroring Overview
- Mirroring Configuration
- Displaying and Maintaining Port Mirroring
- Mirroring Configuration Examples

Mirroring Overview

Mirroring is to duplicate packets from a port to another port connected with a data monitoring device for network monitoring and diagnosis.

The port where packets are duplicated is called the source mirroring port or monitored port and the port to which duplicated packets are sent is called the destination mirroring port or the monitor port, as shown in the following figure.

Figure 1-1 Mirroring



The Switch 4500 series support three types of port mirroring:

- Local Port Mirroring
- Remote Port Mirroring
- Traffic Mirroring

They are described in the following sections.

Local Port Mirroring

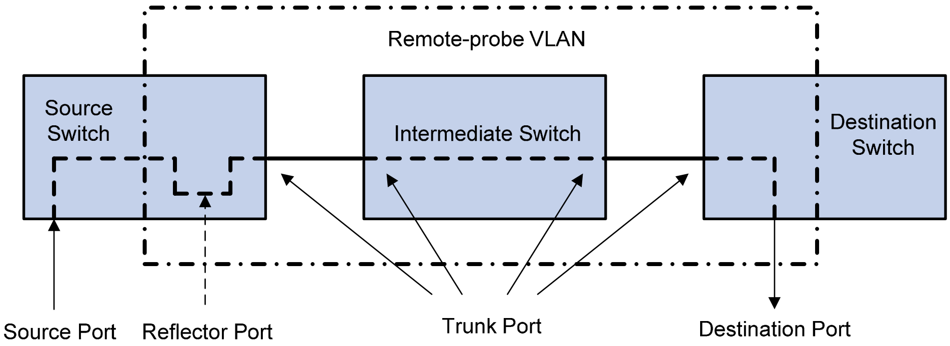
In local port mirroring, packets passing through one or more source ports of a device are copied to the destination port on the same device for packet analysis and monitoring. In this case, the source ports and the destination port must be located on the same device.

Remote Port Mirroring

Remote port mirroring does not require the source and destination ports to be on the same device. The source and destination ports can be located on multiple devices across the network. This allows an administrator to monitor traffic on remote devices conveniently.

To implement remote port mirroring, a special VLAN, called remote-probe VLAN, is used. All mirrored packets are sent from the reflector port of the source switch to the monitor port on the destination switch through the remote-probe VLAN. Figure 1-2 illustrates the implementation of remote port mirroring.

Figure 1-2 Remote port mirroring application



The switches involved in remote port mirroring function as follows:

- Source switch

The source switch is the device where the monitored port is located. It copies traffic passing through the monitored port to the reflector port. The reflector port then transmits the traffic to an intermediate switch (if any) or destination switch through the remote-probe VLAN.

- Intermediate switch

Intermediate switches are switches between the source switch and destination switch on the network. An intermediate switch forwards mirrored traffic flows to the next intermediate switch or the destination switch through the remote-probe VLAN. No intermediate switch is present if the source and destination switches directly connect to each other.

- Destination switch

The destination switch is where the monitor port is located. The destination switch forwards the mirrored traffic flows it received from the remote-probe VLAN to the monitoring device through the destination port.

Table 1-1 describes how the ports on various switches are involved in the mirroring operation.

Table 1-1 Ports involved in the mirroring operation

Switch	Ports involved	Function
Source switch	Source port	Port monitored. It copies packets to the reflector port through local port mirroring. There can be more than one source port.
	Reflector port	Receives packets from the source port and broadcasts the packets in the remote-probe VLAN.
	Trunk port	Sends mirrored packets to the intermediate switch or the destination switch.

Switch	Ports involved	Function
Intermediate switch	Trunk port	Sends mirrored packets to the destination switch. Two trunk ports are necessary for the intermediate switch to connect the devices at the source switch side and the destination switch side.
Destination switch	Trunk port	Receives remote mirrored packets.
	Destination port	Receives packets forwarded from the trunk port and transmits the packets to the data detection device.

Caution

- Do not configure a default VLAN, a management VLAN, or a dynamic VLAN as the remote-probe VLAN.
- Configure all ports connecting the devices in the remote-probe VLAN as trunk ports, and ensure the Layer 2 connectivity from the source switch to the destination switch over the remote-probe VLAN.
- Do not configure a Layer 3 interface for the remote-probe VLAN, run other protocol packets, or carry other service packets on the remote-prove VLAN and do not use the remote-prove VLAN as the voice VLAN and protocol VLAN; otherwise, remote port mirroring may be affected.

Traffic Mirroring

Traffic mirroring uses ACL to monitor traffic that matches certain criteria on a specific port. Unlike port mirroring where all inbound/outbound traffic passing through a port is monitored, traffic mirroring provides a finer monitoring granularity. For detailed configuration about traffic mirroring, refer to *QoS-QoS Profile Operation*.

Mirroring Configuration

Complete the following tasks to configure mirroring:

Task	Remarks
Configuring Local Port Mirroring	Optional
Configuring Remote Port Mirroring	Optional

Note

On a Switch 4500, only one destination port for local port mirroring and only one reflector port can be configured, and the two types of ports cannot both exist.

Configuring Local Port Mirroring

Configuration prerequisites

- The source port is determined and the direction in which the packets are to be mirrored is determined.
- The destination port is determined.

Configuration procedure

Follow these steps to configure port mirroring on Switch 4500 series:

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="2">Create a port mirroring group</td><td>mirroring-group group-id local</td><td>Required</td></tr>
<tr><td rowspan="4">Configure the source port for the port mirroring group</td><td>In system view</td><td>mirroring-group group-id mirroring-port mirroring-port-list { both | inbound | outbound }</td><td rowspan="4">Use either approach
You can configure multiple source ports at a time in system view, or you can configure the source port in specific port view. The configurations in the two views have the same effect.</td></tr>
<tr><td rowspan="3">In port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>mirroring-group group-id mirroring-port { both | inbound | outbound }</td></tr>
<tr><td>quit</td></tr>
<tr><td rowspan="3">Configure the destination port for the port mirroring group</td><td>In system view</td><td>mirroring-group group-id monitor-port monitor-port-id</td><td rowspan="3">Use either approach
The configurations in the two views have the same effect.</td></tr>
<tr><td rowspan="2">In port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>mirroring-group group-id monitor-port</td></tr>
</table>

When configuring local port mirroring, note that:

- You need to configure the source and destination ports for the local port mirroring to take effect.
- The source port and the destination port cannot be a fabric port or a member port of an existing mirroring group; besides, the destination port cannot be a member port of an aggregation group or a port enabled with LACP or STP.

Configuring Remote Port Mirroring

Note

A Switch 4500 can serve as a source switch, an intermediate switch, or a destination switch in a remote port mirroring networking environment.

Configuration on a switch acting as a source switch

1) Configuration prerequisites

- The source port, the reflector port, and the remote-probe VLAN are determined.
- Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.
- The direction of the packets to be monitored is determined.

2) Configuration procedure

Follow these steps to perform configurations on the source switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a VLAN and enter the VLAN view	**vlan** *vlan-id*	*vlan-id* is the ID of the remote-probe VLAN.
Configure the current VLAN as the remote-probe VLAN	**remote-probe vlan enable**	Required
Return to system view	**quit**	—
Enter the view of the Ethernet port that connects to the intermediate switch or destination switch	**interface** *interface-type interface-number*	—
Configure the current port as trunk port	**port link-type trunk**	Required By default, the port type is Access.
Configure the trunk port to permit packets from the remote-probe VLAN	**port trunk permit vlan** *remote-probe-vlan-id*	Required
Return to system view	**quit**	—
Create a remote source mirroring group	**mirroring-group** *group-id* **remote-source**	Required
Configure source port(s) for the remote source mirroring group	**mirroring-group** *group-id* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }	Required
Configure the reflector port for the remote source mirroring group	**mirroring-group** *group-id* **reflector-port** *reflector-port*	Required
Configure the remote-probe VLAN for the remote source mirroring group	**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*	Required

When configuring the source switch, note that:

- All ports of a remote source mirroring group are on the same device. Each remote source mirroring group can be configured with only one reflector port.
- The reflector port cannot be a member port of an existing mirroring group, a fabric port, a member port of an aggregation group, or a port enabled with LACP or STP. It must be an access port and

cannot be configured with functions like VLAN-VPN, port loopback detection, packet filtering, QoS, port security, and so on.

- You cannot modify the duplex mode, port rate, and MDI attribute of a reflector port.
- Only an existing static VLAN can be configured as the remote-probe VLAN. To remove a remote-probe VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.
- Do not configure a port connecting the intermediate switch or destination switch as the mirroring source port. Otherwise, traffic disorder may occur in the network.

Configuration on a switch acting as an intermediate switch

1) Configuration prerequisites

- The trunk ports and the remote-probe VLAN are determined.
- Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.

2) Configuration procedure

Follow these steps to perform configurations on the intermediate switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	*vlan-id* is the ID of the remote-probe VLAN.
Configure the current VLAN as the remote-probe VLAN	**remote-probe vlan enable**	Required
Return to system view	**quit**	—
Enter the view of the Ethernet port connecting to the source switch, destination switch or other intermediate switch	**interface** *interface-type interface-number*	—
Configure the current port as trunk port	**port link-type trunk**	Required By default, the port type is Access.
Configure the trunk port to permit packets from the remote-probe VLAN	**port trunk permit vlan** *remote-probe-vlan-id*	Required

Note that a Switch 4500 acting as the intermediate switch in remote port mirroring networking does not support bidirectional packet mirroring (the **both** keyword).

Configuration on a switch acting as a destination switch

1) Configuration prerequisites

- The destination port and the remote-probe VLAN are determined.
- Layer 2 connectivity is ensured between the source and destination switches over the remote-probe VLAN.

2) Configuration procedure

Follow these steps to configure remote port mirroring on the destination switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a VLAN and enter VLAN view	**vlan** *vlan-id*	*vlan-id* is the ID of the remote-probe VLAN.
Configure the current VLAN as a remote-probe VLAN	**remote-probe vlan enable**	Required
Return to system view	**quit**	—
Enter the view of the Ethernet port connecting to the source switch or an intermediate switch	**interface** *interface-type interface-number*	—
Configure the current port as trunk port	**port link-type trunk**	Required By default, the port type is Access.
Configure trunk port to permit packets from the remote-probe VLAN	**port trunk permit vlan** *remote*-probe-*vlan-id*	Required
Return to system view	**quit**	—
Create a remote destination mirroring group	**mirroring-group** *group-id* **remote-destination**	Required
Configure the destination port for the remote destination mirroring group	**mirroring-group** *group-id* **monitor-port** *monitor-port*	Required
Configure the remote-probe VLAN for the remote destination mirroring group	**mirroring-group** *group-id* **remote-probe vlan** *remote-probe-vlan-id*	Required

When configuring a destination switch, note that:

- A Switch 4500 acting as the destination switch in remote port mirroring networking does not support bidirectional packet mirroring (the **both** keyword).
- The destination port of remote port mirroring cannot be a member port of an existing mirroring group, a fabric port, a member port of an aggregation group, or a port enabled with LACP or STP.
- Only an existing static VLAN can be configured as the remote-probe VLAN. To remove a remote-probe VLAN, you need to restore it to a normal VLAN first. A remote port mirroring group gets invalid if the corresponding remote port mirroring VLAN is removed.

Displaying and Maintaining Port Mirroring

To do…	Use the command…	Remarks
Display port mirroring configuration on a Switch 4500	**display mirroring-group** { *group-id* | **all** | **local** | **remote-destination** | **remote-source** }	Available in any view

Mirroring Configuration Examples

Local Port Mirroring Configuration Example

Network requirements

The departments of a company connect to each other through Switch 4500 series:

- Research and Development (R&D) department is connected to Switch C through Ethernet 1/0/1.
- Marketing department is connected to Switch C through Ethernet 1/0/2.
- Data detection device is connected to Switch C through Ethernet 1/0/3

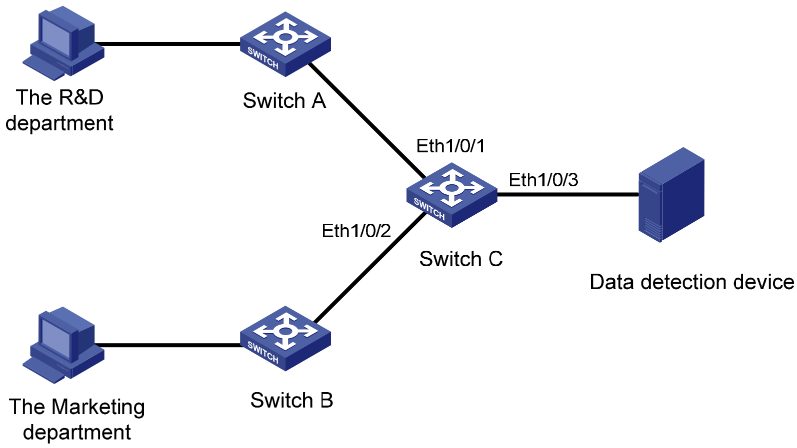
The administrator wants to monitor the packets received on and sent from the R&D department and the marketing department through the data detection device.

Use the local port mirroring function to meet the requirement. Perform the following configurations on Switch C.

- Configure Ethernet 1/0/1 and Ethernet 1/0/2 as mirroring source ports.
- Configure Ethernet 1/0/3 as the mirroring destination port.

Network diagram

Figure 1-3 Network diagram for local port mirroring



Configuration procedure

Configure Switch C:

Create a local mirroring group.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
```

Configure the source ports and destination port for the local mirroring group.

```
[Sysname] mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/2 both
[Sysname] mirroring-group 1 monitor-port Ethernet 1/0/3
```

Display configuration information about local mirroring group 1.

```
[Sysname] display mirroring-group 1
mirroring-group 1:
    type: local
    status: active
    mirroring port:
```

```
    Ethernet1/0/1  both
    Ethernet1/0/2  both
monitor port: Ethernet1/0/3
```

After the configurations, you can monitor all packets received on and sent from the R&D department and the marketing department on the data detection device.

Remote Port Mirroring Configuration Example

Network requirements

The departments of a company connect to each other through Switch 4500 series:

- Switch A, Switch B, and Switch C are Switch 4500 series.
- Department 1 is connected to Ethernet 1/0/1 of Switch A.
- Department 2 is connected to Ethernet 1/0/2 of Switch A.
- Ethernet 1/0/3 of Switch A connects to Ethernet 1/0/1 of Switch B.
- Ethernet 1/0/2 of Switch B connects to Ethernet 1/0/1 of Switch C.
- The data detection device is connected to Ethernet 1/0/2 of Switch C.

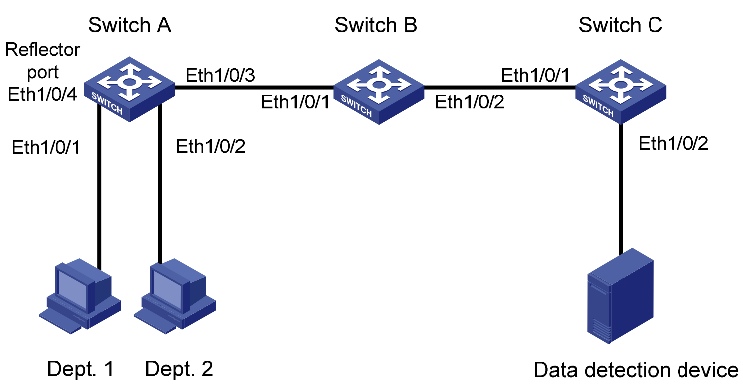
The administrator wants to monitor the packets sent from Department 1 and 2 through the data detection device.

Use the remote port mirroring function to meet the requirement. Perform the following configurations:

- Use Switch A as the source switch, Switch B as the intermediate switch, and Switch C as the destination switch.
- On Switch A, create a remote source mirroring group, configure VLAN 10 as the remote-probe VLAN, ports Ethernet 1/0/1 and Ethernet 1/0/2 as the source ports, and port Ethernet 1/0/4 as the reflector port.
- On Switch B, configure VLAN 10 as the remote-probe VLAN.
- Configure Ethernet 1/0/3 of Switch A, Ethernet 1/0/1 and Ethernet 1/0/2 of Switch B, and Ethernet 1/0/1 of Switch C as trunk ports, allowing packets of VLAN 10 to pass.
- On Switch C, create a remote destination mirroring group, configure VLAN 10 as the remote-probe VLAN, and configure Ethernet 1/0/2 connected with the data detection device as the destination port.

Network diagram

Figure 1-4 Network diagram for remote port mirroring



Configuration procedure

1) Configure the source switch (Switch A)

Create remote source mirroring group 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-source
```

Configure VLAN 10 as the remote-probe VLAN.

```
[Sysname] vlan 10
[Sysname-vlan10] remote-probe vlan enable
[Sysname-vlan10] quit
```

Configure the source ports, reflector port, and remote-probe VLAN for the remote source mirroring group.

```
[Sysname] mirroring-group 1 mirroring-port Ethernet 1/0/1 Ethernet 1/0/2 inbound
[Sysname] mirroring-group 1 reflector-port Ethernet 1/0/4
[Sysname] mirroring-group 1 remote-probe vlan 10
```

Configure Ethernet 1/0/3 as trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] port link-type trunk
[Sysname-Ethernet1/0/3] port trunk permit vlan 10
[Sysname-Ethernet1/0/3] quit
```

Display configuration information about remote source mirroring group 1.

```
[Sysname] display mirroring-group 1
mirroring-group 1:
    type: remote-source
    status: active
    mirroring port:
        Ethernet1/0/1  inbound
        Ethernet1/0/2  inbound
    reflector port: Ethernet1/0/4
    remote-probe vlan: 10
```

2) Configure the intermediate switch (Switch B)

Configure VLAN 10 as the remote-probe VLAN.

```
<Sysname> system-view
[Sysname] vlan 10
[Sysname-vlan10] remote-probe vlan enable
[Sysname-vlan10] quit
```

Configure Ethernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] port link-type trunk
[Sysname-Ethernet1/0/1] port trunk permit vlan 10
[Sysname-Ethernet1/0/1] quit
```

Configure Ethernet 1/0/2 as the trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] port link-type trunk
```

```
[Sysname-Ethernet1/0/2] port trunk permit vlan 10
```

3) Configure the destination switch (Switch C)

Create remote destination mirroring group 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 remote-destination
```

Configure VLAN 10 as the remote-probe VLAN.

```
[Sysname] vlan 10
[Sysname-vlan10] remote-probe vlan enable
[Sysname-vlan10] quit
```

Configure the destination port and remote-probe VLAN for the remote destination mirroring group.

```
[Sysname] mirroring-group 1 monitor-port Ethernet 1/0/2
[Sysname] mirroring-group 1 remote-probe vlan 10
```

Configure Ethernet 1/0/1 as the trunk port, allowing packets of VLAN 10 to pass.

```
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] port link-type trunk
[Sysname-Ethernet1/0/1] port trunk permit vlan 10
[Sysname-Ethernet1/0/1] quit
```

Display configuration information about remote destination mirroring group 1.

```
[Sysname] display mirroring-group 1
mirroring-group 1:
    type: remote-destination
    status: active
    monitor port: Ethernet1/0/2
    remote-probe vlan: 10
```

After the configurations, you can monitor all packets sent from Department 1 and 2 on the data detection device.

Table of Contents

1 XRN Fabric Configuration

When configuring XRN fabric, go to these sections for information you are interested in:

- Introduction to XRN
- XRN Fabric Configuration
- Displaying and Maintaining XRN Fabric
- XRN Fabric Configuration Example

Introduction to XRN

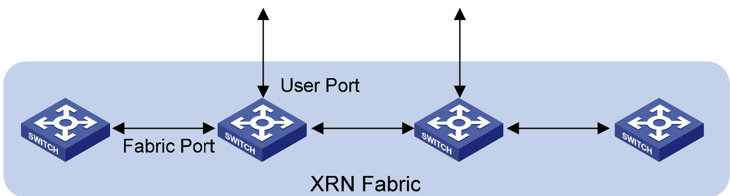
Expandable Resilient Networking (XRN), a feature particular to 3Com Switch 4500 series switches, is a new technology for building the core of a network. This feature allows you to build an XRN fabric by interconnecting several Switch 4500 series switches to provide more ports for network devices and improve the reliability of your network.

Establishment of an XRN Fabric

Topology and connections of an XRN fabric

An XRN fabric typically has a bus topology structure. As shown in Figure 1-1, each switch has two ports connected with two other switches in the fabric, but the switches at both ends of the bus have only one port connected. These ports are called fabric ports in general, a left port and a right port respectively; the other ports, which are available for connections with users or devices outside the fabric, are called user ports.

Figure 1-1 A schematic diagram of an XRN fabric

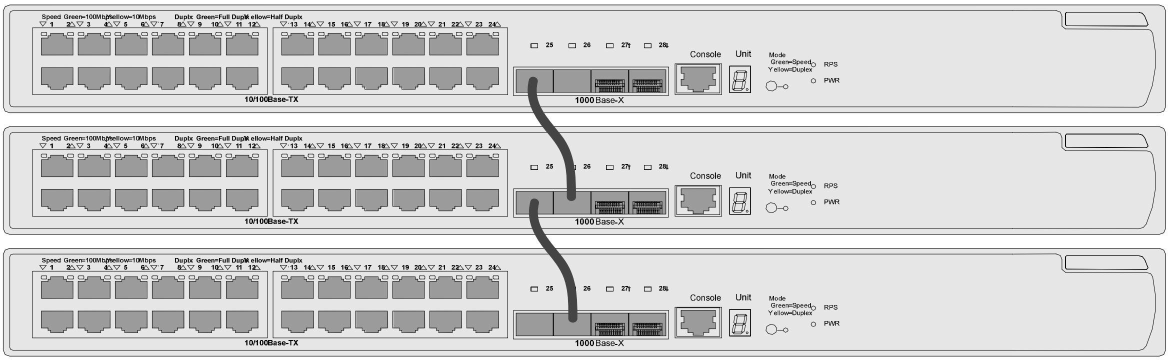


A correctly built XRN fabric features the following:

- Multiple Switch 4500 series switches are interconnected through their fabric ports.
- Given a switch, its left port is connected to the right port of another switch, and its right port is connected to the left port of a third one.

Port connection mode for Switch 4500 series bus topology XRN fabric is shown in Figure 1-2.

Figure 1-2 Port connection mode for Switch 4500 series bus topology XRN fabric



Fabric ports

On a Switch 4500-26Port (Switch 4500-50Port) series Ethernet switch, only four GigabitEthernet ports can be configured as fabric ports. If not used for fabric connection, these four ports can be used as general data ports. The four ports fall into two groups according to their port numbers:

- GigabitEthernet 1/0/25(49) and GigabitEthernet 1/0/26(50) form the first group.
- GigabitEthernet 1/0/27(51) and GigabitEthernet 1/0/28(52) form the second group.

Only one group of ports can be configured as fabric ports at a time. Given a group, either GigabitEthernet 1/0/25(49) or GigabitEthernet 1/0/27(51) can be configured as the left fabric port, and either GigabitEthernet 1/0/26(50) or GigabitEthernet 1/0/28(52) can be configured as the right fabric port.

Once you configure a port as a fabric port, the group that comprises this fabric port becomes the fabric port group, and you cannot configure a port in the other group as a fabric port. For example, once you configure GigabitEthernet 1/0/25 as a fabric port, this port automatically becomes the left port and the first group becomes the fabric port group.

Note

The system does not require a consistency in the fabric port groups between different switches. That is, the left fabric port in the first group of a switch can be connected to the right fabric port in the second group of the peer switch.

FTM

As the basis of the XRN function, the Fabric Topology Management (FTM) program manages and maintains the entire topology of a fabric.

With fabric ports configured, the FTM program releases information of the device through the fabric ports. The device information includes Unit ID, CPU MAC, device type ID, fabric port information, and all fabric configuration information. The device information is released in the discovery packet (DISC).

After receiving the packet, the peer device will analyze the packet. A device can form a fabric with the peer or join a fabric only when the following conditions are met.

- The number of the existing devices in the fabric does not reach the maximum number of devices allowed by the fabric (up to eight devices can form a fabric).
- The fabric name of the device and the existing devices in the fabric are the same.
- The software version of the device is the same as that of the existing devices in the fabric.
- The device passes the security authentication if security authentication is enabled on the device or in the fabric, that is, the same authentication mode and password are configured on the device and the existing devices in the fabric.

XRN fabric detection

Forming a fabric requires a high consistency of connection modes between the devices and device information. Without all the requirements for forming a fabric being met, a fabric cannot be formed.

The FTM program detects the necessary conditions for forming a fabric one by one and displays the detection results. You can use the **display ftm information** command to view the detection information for the fabric, checking the running status of the fabric or analyzing the problems. Table 1-1 lists the status and solution of the problems.

Table 1-1 Status and solution

<table>
<tr><th>Status</th><th colspan="2">Analysis</th><th>Solution</th></tr>
<tr><td>normal</td><td colspan="2" rowspan="3">—</td><td rowspan="3">These three kinds of information do not mean a device or a fabric operates improperly. No measure is needed for any of them.</td></tr>
<tr><td>temporary</td></tr>
<tr><td>redundance port</td></tr>
<tr><td rowspan="3">connection error</td><td rowspan="3">Indicates three kinds of port matching errors may occur.</td><td>Two fabric ports of the same device (that is, the right port and the left port) are connected.</td><td>Pull out one end of the cable and connect it to a fabric port of another switch.</td></tr>
<tr><td>The left and right fabric ports of the devices are not connected in a crossed way.</td><td>Connect the left and right ports of two devices in a crossed way.</td></tr>
<tr><td>A fabric port of the local switch is connected to a non-fabric port, or is connected to a fabric port that does not have fabric port function enabled.</td><td>Check the types of the two interconnected ports on two sides. Make sure a fabric port is only connected to ports of the same type and the fabric ports on both sides are enabled with the fabric port function.</td></tr>
<tr><td>reached max units</td><td colspan="2">The maximum number of units allowed by the current fabric is reached. You will fail to add new devices to the fabric in this case.</td><td>Remove the new device or existing devices in the fabric.</td></tr>
<tr><td>different system name</td><td colspan="2">The fabric name of the device directly connected to the switch and the existing fabric name of the fabric are not the same.</td><td>Modify the fabric name of the new device to be that of the fabric.</td></tr>
<tr><td>different product version</td><td colspan="2">The software version of the directly connected device and that of the current device are not the same.</td><td>Update the software version to make sure the software version of the new device is the same as that of the fabric.</td></tr>
<tr><td>auth failure</td><td colspan="2">The XRN fabric authentication modes configured for the local device and that</td><td>Configure the XRN fabric authentication modes and the</td></tr>
</table>

Status	Analysis	Solution
	of the fabric are not the same, or the password configured does not match.	passwords for the local device and the fabric as the same.

How XRN Works

When a fabric is established, the devices determine their respective roles in the fabric by comparing their CPU MAC addresses. The device with the lowest CPU MAC address is elected as the master and the other devices are slaves.

After the election, the fabric can operate normally. The following three functions of XRN can provide simple configuration mode, enhanced network performance and perfect redundancy backup mechanism for users.

DDM

DDM is a new device management mode provided by XRN. In normal cases, a fabric can be considered as a single device. You can manage the entire fabric by logging onto any device in the fabric with different logging modes. The devices in the fabric synchronize their configurations by exchanging packets, thus ensuring stability of the fabric.

FTM program uses Unit ID, or device ID to distinguish between the devices in a fabric when you manage them. On initialization of the XRN function, each device considers its Unit ID as 1 and after a fabric connection is established, the FTM program automatically re-numbers the devices or you can manually configure the Unit ID of them.

The master in a fabric collects the newest configurations of the user and the slaves periodically synchronize the configurations from the master. In this way, the entire fabric can operate with the same configurations.

DLA

As a new link aggregation mode, DLA can improve fault tolerance and redundancy backup of user networks.

Link aggregation enables you to configure ports on the same device as an aggregation port group, avoiding network interruptions resulted from single port failure. Based on link aggregation, DLA provides a more reliable solution, with which you can select ports on different devices to form an aggregation port group. In this way, single port failure can be avoided and network reliability can be greatly improved, because the fabric can communicate with the destination network through ports on other devices in case a single device fails.

XRN Fabric Configuration

XRN Fabric Configuration Task List

Complete the following tasks to configure XRN fabric:

Task	Remarks
Specifying the Fabric Port of a Switch	Required
Specifying the VLAN Used to Form an XRN	Optional

Task	Remarks
Fabric	
Setting a Unit ID for a Switch	Optional
Assigning a Unit Name to a Switch	Optional
Assigning an XRN Fabric Name to a Switch	Optional
Setting the XRN Fabric Authentication Mode	Optional

Specifying the Fabric Port of a Switch

You can specify the fabric port of a switch in either system view or Ethernet interface view.

Configurations in system view

Follow these steps to specify a fabric port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify the fabric port of a switch	**fabric-port** *interface-type interface-number* **enable**	Required Not specified by default

Configurations in Ethernet interface view

Follow these steps to specify a fabric port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet interface view	**interface** *interface-type interface-number*	—
Specify the current port as the fabric port of a switch	**port link-type xrn-fabric**	Required No port is specified as the fabric port by default.

Note

- Establishing an XRN system requires a high consistency of the configuration of each device. Hence, before you enable the fabric port, do not perform any configuration for the port, and do not configure some functions that affect the XRN for other ports or globally. Otherwise, you cannot enable the fabric port. For detailed restrictions refer to the error information output by devices.
- When you have enabled fabric port function for a fabric port group, if you need to change the fabric port group, you must disable the fabric function of the current fabric port group before you configure another group. Otherwise, the system will prompt that the current fabric port group is in use, you cannot change the fabric port group.
- As shutting down a fabric port directly may cause the fabric to be split and error messages, do not perform such operations.
- To split a fabric, you can simply remove the cables used to form the fabric or disable the fabric using the **undo fabric-port enable** command.
- You can shut down/bring up a port after you disable the fabric feature on the port.
- If you need to configure an XRN fabric as a DHCP relay or DHCP client, configure the UDP Helper function in the fabric at the same time to ensure that the client can successfully obtain an IP address. (Since this configuration can be automatically synchronized to the entire fabric, you can perform it on only one unit.) For the configuration of the UDP Helper function, refer to the UDP Helper part in this manual.
- After you use the **port link-type xrn-fabric** command to specify a port as the fabric port, you cannot use the **port link-type** command to change the port to a port of other types. You must use the **undo fabric-port** command first to disable the fabric port function of the port to change the port type.

Specifying the VLAN Used to Form an XRN Fabric

When the devices in an XRN fabric are transmitting XRN data, to avoid it being sent to other non fabric ports, the data should be transmitted in a specified VLAN. You can specify the VLAN used to transmit XRN data.

Follow these steps to specify the VLAN used to form an XRN fabric:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify the VLAN used to form an XRN fabric	**ftm fabric-vlan** *vlan-id*	Required By default, the VLAN used to form the XRN fabric is VLAN 4093

Caution

You cannot specify an existing VLAN to form an XRN fabric; otherwise, your configuration fails.

Setting a Unit ID for a Switch

On the switches that support automatic numbering, FTM will automatically number the switches to constitute an XRN fabric by default, so that each switch has a unique unit ID in the fabric. You can use the command in the following table to set unit IDs for switches. Make sure to set different unit IDs for different switches in an XRN fabric. Otherwise, FTM will automatically number the switches with the same unit ID.

Follow these steps to set a unit ID for a switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set a unit ID for the switch	**change self-unit to** { *unit-id* | **auto-numbering** }	Optional By default, the unit ID of a switch that belongs to no XRN fabric is 1. The unit ID of a switch belonging to an XRN fabric is assigned by FTM. Unit ID ranges from 1 to 8.

Note

If you do not configure the fabric port, you cannot change the unit ID of the local switch.

After an XRN fabric is established, you can use the following command to change the unit IDs of the switches in the XRN fabric.

Follow these steps to set a unit ID to a new value:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set a unit ID to a new value	**change unit-id** *unit-id1* **to** { *unit-id2* | **auto-numbering** }	Optional

Note

- Unit IDs in an XRN fabric are not always arranged in order of 1 to 8.
- Unit IDs of an XRN fabric can be inconsecutive.

After you change the unit ID of switches, the following operations are performed.

- If the modified unit ID does not exist in the XRN fabric, the system sets its priority to 5 and saves it in the unit Flash memory.
- If the modified unit ID is an existing one, the system prompts you to confirm if you really want to change the unit ID. If you choose to change it, the existing unit ID is replaced and the priority is set to 5. Then you can use the **fabric save-unit-id** command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.

- If **auto-numbering** is selected, the system sets the unit priority to 10. You can use the **fabric save-unit-id** command to save the modified unit ID into the unit Flash memory and clear the information about the existing one.

Note

Priority is the reference for FTM program to perform automatic numbering. The value of priority can be 5 or 10. Priority 5 means the switch adopts manual numbering, and priority 10 means the switch adopts automatic numbering. Manual numbering has a higher priority than automatic numbering.

After the configuration of numbering, you can use the following command in the table to save the local unit ID in the unit Flash memory. When you restart the switch, it can load the unit ID configuration automatically.

Follow these steps to save the unit ID of each unit in the XRN fabric:

To do…	Use the command…	Remarks
Save the unit ID of each unit in the XRN fabric	**fabric save-unit-id**	Optional

Assigning a Unit Name to a Switch

Follow these steps to assign a unit name to a switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Assign a unit name to a switch	**set unit** *unit-id* **name** *unit-name*	Required

Assigning an XRN Fabric Name to a Switch

Only the switches with the same XRN fabric name can form an XRN fabric.

Follow these steps to assign a fabric name to a switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Assign a fabric name to the switch	**sysname** *sysname*	Optional By default, the XRN fabric name is 4500.

Setting the XRN Fabric Authentication Mode

Only the switches with the same XRN fabric authentication mode can form an XRN fabric.

Follow these steps to set the XRN fabric authentication mode for a switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the XRN fabric authentication mode for the switch	**xrn-fabric authentication-mode** { **simple** *password* | **md5** *key* }	Optional By default, no authentication mode is set on a switch.

Note

When an XRN fabric operates normally, you can regard the whole fabric as a single device and perform configuration on it. Multiple switches constitute an XRN fabric. Therefore, data transmission and simultaneous program execution among the switches may cause the XRN fabric in a busy situation. When you configure the XRN fabric, you may receive a prompt "Fabric system is busy, please try later…" which indicates the fabric system does not perform your configuration properly. In this case, you need to verify your previous configuration or perform your configuration again.

Displaying and Maintaining XRN Fabric

To do…	Use the command…	Remarks
Display the information about an XRN fabric	**display xrn-fabric** [**port**]	Available in any view
Display the topology information of an XRN fabric	**display ftm** { **information** | **topology-database** }	
Clear the FTM statistics	**reset ftm statistics**	Available in user view

XRN Fabric Configuration Example

Network Requirements

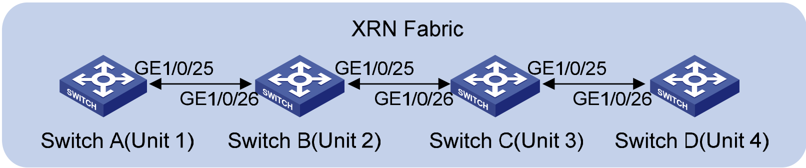
Configure unit ID, unit name, XRN fabric name, and authentication mode for four switches to enable them to form an XRN fabric as shown in Figure 1-3.

The configuration details are as follows:

- Unit IDs: 1, 2, 3, 4
- Unit names: unit 1, unit 2, unit 3, unit 4
- Fabric name: hello
- Authentication mode: simple password
- Password: welcome

Network Diagram

Figure 1-3 Network diagram for forming an XRN fabric



Configuration Procedure

1) Configure Switch A.

Configure fabric ports.

```
<Sysname> system-view
[Sysname] fabric-port GigabitEthernet1/0/25 enable
```

Configure the unit name as **Unit 1**.

```
[Sysname] set unit 1 name Unit1
```

Configure the fabric name as **hello**.

```
[Sysname] sysname hello
```

Configure the fabric authentication mode as **simple** and the password as **welcome**.

```
[hello] xrn-fabric authentication-mode simple welcome
```

2) Configure Switch B.

Configure fabric ports.

```
<Sysname> system-view
[Sysname] fabric-port GigabitEthernet1/0/25 enable
[Sysname] fabric-port GigabitEthernet1/0/26 enable
```

Set the unit ID to 2.

```
[Sysname] change unit-id 1 to 2
```

Configure the unit name as **Unit 2**.

```
[Sysname] set unit 1 name unit2
```

Configure the fabric name as **hello**.

```
[Sysname] sysname hello
```

Configure the fabric authentication mode as **simple** and the password as **welcome**.

```
[hello] xrn-fabric authentication-mode simple welcome
```

3) Configure Switch C.

Configure fabric ports.

```
<Sysname> system-view
[Sysname] fabric-port GigabitEthernet1/0/25 enable
[Sysname] fabric-port GigabitEthernet1/0/26 enable
```

Set the unit ID to 3.

```
[Sysname] change unit-id 1 to 3
```

Configure the unit name as **Unit 3**.

```
[Sysname] set unit 1 name unit3
```

Configure the fabric name as **hello**.

```
[Sysname] sysname hello
```

Configure the fabric authentication mode as **simple** and the password as **welcome**.

```
[hello] xrn-fabric authentication-mode simple welcome
```

4) Configure Switch D.

Configure fabric ports.

```
<Sysname> system-view
[Sysname] fabric-port GigabitEthernet1/0/26 enable
```

Set the unit ID to 4.

```
[Sysname] change unit-id 1 to 4
```

Configure the unit name as **Unit 4**.

```
[Sysname] set unit 1 name Unit4
```

Configure the fabric name as **hello**.

```
[Sysname] sysname hello
```

Configure the fabric authentication mode as **simple** and the password as **welcome**.

```
[hello] xrn-fabric authentication-mode simple welcome
```

Table of Contents

1 Cluster

When configuring cluster, go to these sections for information you are interested in:

- Cluster Overview
- Cluster Configuration Task List
- Displaying and Maintaining Cluster Configuration
- Cluster Configuration Examples

Cluster Overview

Introduction to HGMP

A cluster contains a group of switches. Through cluster management, you can manage multiple geographically dispersed in a centralized way.

Cluster management is implemented through Huawei Group Management Protocol (HGMP). HGMP version 2 (HGMPv2) is used at present.

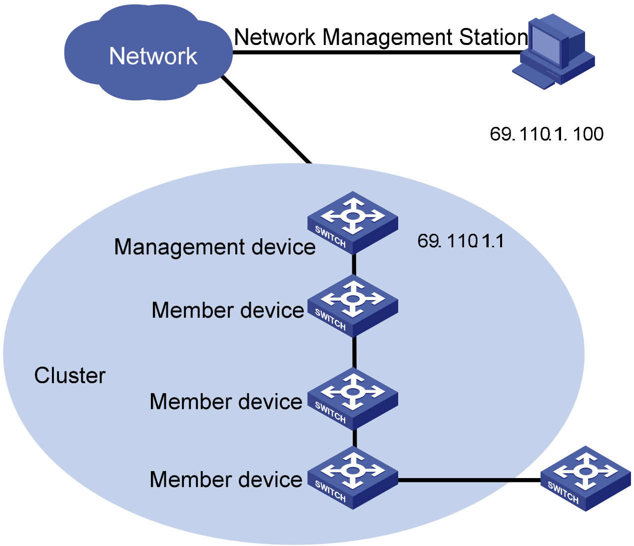
A switch in a cluster plays one of the following three roles:

- Management device
- Member device
- Candidate device

A cluster comprises of a management device and multiple member devices. To manage the devices in a cluster, you need only to configure an external IP address for the management switch. Cluster management enables you to configure and manage remote devices in batches, reducing the workload of the network configuration. Normally, there is no need to configure external IP addresses for member devices.

Figure 1-1 illustrates a cluster implementation.

Figure 1-1 A cluster implementation



HGMP V2 has the following advantages:

- It eases the configuration and management of multiple switches: You just need to configure a public IP address for the management device instead of for all the devices in the cluster; and then you can configure and manage all the member devices through the management device without the need to log onto them one by one.
- It provides the topology discovery and display function, which assists in monitoring and maintaining the network.
- It allows you to configure and upgrade multiple switches at the same time.
- It enables you to manage your remotely devices conveniently regardless of network topology and physical distance.
- It saves IP address resource.

Roles in a Cluster

The switches in a cluster play different roles according to their functions and status. You can specify the role a switch plays. A switch in a cluster can also switch to other roles under specific conditions.

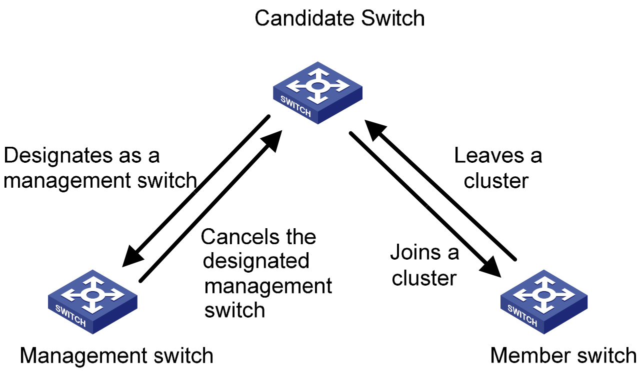
As mentioned above, the three cluster roles are management device, member device, and candidate device.

Table 1-1 Description on cluster roles

Role	Configuration	Function
Management device	Configured with a external IP address	• Provides an interface for managing all the switches in a cluster • Manages member devices through command redirection, that is, it forwards the commands intended for specific member devices. • Discovers neighbors, collects the information about network topology, manages and maintains the cluster. Management device also supports FTP server and SNMP host proxy. • Processes the commands issued by users through the public network
Member device	Normally, a member device is not assigned an external IP address	• Members of a cluster • Discovers the information about its neighbors, processes the commands forwarded by the management device, and reports log. The member devices of a luster are under the management of the management device.
Candidate device	Normally, a candidate device is not assigned an external IP address	Candidate device refers to the devices that do not belong to any clusters but are cluster-capable.

Figure 1-2 illustrates the state machine of cluster role.

Figure 1-2 State machine of cluster role



- A candidate device becomes a management device when you create a cluster on it. Note that a cluster must have one (and only one) management device. On becoming a management device, the device collects network topology information and tries to discover and determine candidate devices, which can then be added to the cluster through configurations.

- A candidate device becomes a member device after being added to a cluster.
- A member device becomes a candidate device after it is removed from the cluster.
- A management device becomes a candidate device only after the cluster is removed.

Note

After you create a cluster on a Switch 4500 switch, the switch collects the network topology information periodically and adds the candidate switches it finds to the cluster. The interval for a management device to collect network topology information is determined by the NTDP timer. If you do not want the candidate switches to be added to a cluster automatically, you can set the topology collection interval to 0 by using the **ntdp timer** command. In this case, the switch does not collect network topology information periodically.

How a Cluster Works

HGMPv2 consists of the following three protocols:

- Neighbor Discovery Protocol (NDP)
- Neighbor Topology Discovery Protocol (NTDP)
- Cluster

A cluster configures and manages the devices in it through the above three protocols.

Cluster management involves topology information collection and the establishment/maintenance of a cluster. Topology information collection and cluster establishment/maintenance are independent from each other. The former, as described below, starts before a cluster is established.

- All devices use NDP to collect the information about their neighbors, including software version, host name, MAC address, and port name.
- The management device uses NTDP to collect the information about the devices within specific hops and the topology information about the devices. It also determines the candidate devices according to the information collected.
- The management device adds the candidate devices to the cluster or removes member devices from the cluster according to the candidate device information collected through NTDP.

Introduction to NDP

NDP is a protocol used to discover adjacent devices and provide information about them. NDP operates on the data link layer, and therefore it supports different network layer protocols.

NDP is able to discover directly connected neighbors and provide the following neighbor information: device type, software/hardware version, and connecting port. In addition, it may provide the following neighbor information: device ID, port full/half duplex mode, product version, the Boot ROM version and so on.

- An NDP-enabled device maintains an NDP neighbor table. Each entry in the NDP table can automatically ages out. You can also clear the current NDP information manually to have neighbor information collected again.
- An NDP-enabled device regularly broadcasts NDP packet through all its active ports. An NDP packet carries a holdtime field, which indicates how long the receiving devices will keep the NDP

packet data. The receiving devices store the information carried in the NDP packet into the NDP table but do not forward the NDP packet. When they receive another NDP packet, if the information carried in the packet is different from the stored one, the corresponding entry in the NDP table is updated, otherwise only the holdtime of the entry is updated.

Introduction to NTDP

NTDP is a protocol used to collect network topology information. NTDP provides information required for cluster management: it collects topology information about the switches within the specified hop count, so as to provide the information of which devices can be added to a cluster.

Based on the neighbor information stored in the neighbor table maintained by NDP, NTDP on the management device advertises NTDP topology collection requests to collect the NDP information of each device in a specific network range as well as the connection information of all its neighbors. The information collected will be used by the management device or the network management software to implement required functions.

When a member device detects a change on its neighbors through its NDP table, it informs the management device through handshake packets, and the management device triggers its NTDP to perform specific topology collection, so that its NTDP can discover topology changes timely.

The management device collects the topology information periodically. You can also launch an operation of topology information collection by executing related commands. The process of topology information collection is as follows.

- The management device sends NTDP topology collection requests periodically through its NTDP-enabled ports.
- Upon receiving an NTDP topology collection request, the device returns a NTDP topology collection response to the management device and forwards the request to its neighbor devices through its NTDP-enable ports. The topology collection response packet contains the information about the local device and the NDP information about all the neighbor devices.
- The neighbor devices perform the same operation until the NTDP topology collection request is propagated to all the devices within the specified hops.

When an NTDP topology collection request is propagated in the network, it is received and forwarded by large numbers of network devices, which may cause network congestion and the management device busy processing of the NTDP topology collection responses. To avoid such cases, the following methods can be used to control the NTDP topology collection request advertisement speed.

- Configuring the devices not to forward the NTDP topology collection request immediately after they receive an NTDP topology collection request. That is, configure the devices to wait for a period before they forward the NTDP topology collection request.
- Configuring each NTDP-enabled port on a device to forward an NTDP topology collection request after a specific period since the previous port on the device forwards the NTDP topology collection request.

Note

- To implement NTDP, you need to enable NTDP both globally and on specific ports on the management device, and configure NTDP parameters.
- On member/candidate devices, you only need to enable NTDP globally and on specific ports.
- Member and candidate devices adopt the NTDP settings of the management device.

Introduction to Cluster

A cluster must have one and only one management device. Note the following when creating a cluster:

- You need to designate a management device for the cluster. The management device of a cluster is the portal of the cluster. That is, any operations from outside the network intended for the member devices of the cluster, such as accessing, configuring, managing, and monitoring, can only be implemented through the management device.
- The management device of the cluster recognizes and controls all the member devices in the cluster, no matter where they are located in the network and how they are connected.
- The management device collects topology information about all member/candidate devices to provide useful information for you to establish the cluster.
- By collecting NDP/NTDP information, the management device learns network topology, so as to manage and monitor network devices.
- Before performing any cluster-related configuration task, you need to enable the cluster function first.

Note

On the management device, you need to enable the cluster function and configure cluster parameters. On the member/candidate devices, however, you only need to enable the cluster function so that they can be managed by the management device.

Cluster maintenance

1) Adding a candidate device to a cluster

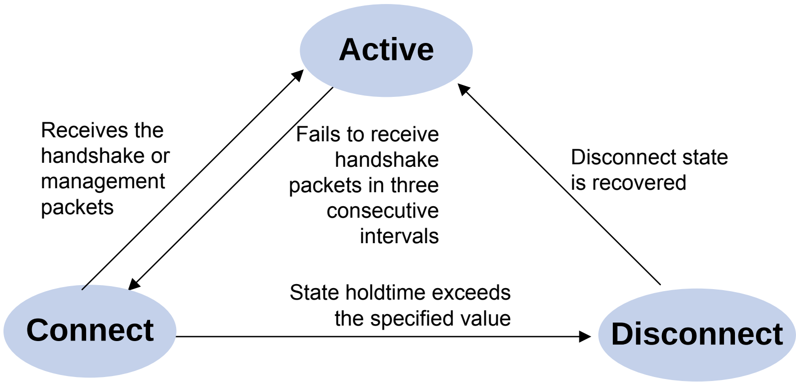
To create a cluster, you need to determine the device to operate as the management device first. The management device discovers and determines candidate devices through NDP and NTDP, and adds them to the cluster. You can also add candidate devices to a cluster manually.

After a candidate device is added to a cluster, the management device assigns a member number and a private IP address (used for cluster management) to it.

2) Communications within a cluster

In a cluster, the management device maintains the connections to the member devices through handshake packets. Figure 1-3 illustrates the state machine of the connection between the management device and a member device.

Figure 1-3 State machine of the connection between the management device and a member device



- After a cluster is created and a candidate device is added to the cluster as a member device, both the management device and the member device store the state information of the member device and mark the member device as Active.
- The management device and the member devices exchange handshake packets periodically. Note that the handshake packets exchanged keep the states of the member devices to be Active and are not responded.
- If the management device does not receive a handshake packet from a member device after a period three times of the interval to send handshake packets, it changes the state of the member device from Active to Connect. Likewise, if a member device fails to receive a handshake packet from the management device after a period three times of the interval to send handshake packets, the state of the member device will also be changed from Active to Connect.
- If the management device receives a handshake packet or management packet from a member device that is in Connect state within the information holdtime, it changes the state of the member device to Active; otherwise, it changes the state of the member device (in Connect state) to Disconnect, in which case the management device considers the member device disconnected. Likewise, if this member device, which is in Connect state, receives a handshake packet or management packet from the management device within the information holdtime, it changes its state to Active; otherwise, it changes its state to Disconnect.
- If the connection between the management device and a member device in Disconnect state is recovered, the member device will be added to the cluster again. After that, the state of the member device will turn to Active both locally and on the management device.

Besides, handshake packets are also used by member devices to inform the management device of topology changes.

Additionally, on the management device, you can configure the FTP server, TFTP server, logging host and SNMP host to be shared by the whole cluster. When a member device in the cluster communicates with an external server, the member device first transmits data to the management device, which then forwards the data to the external server. The management device is the default shared FTP/TFTP server for the cluster; it serves as the shared FTP/TFTP server when no shared FTP/TFTP server is configured for the cluster.

Management VLAN

Management VLAN limits the range of cluster management. Through management VLAN configuration, the following functions can be implemented:

- Enabling the management packets (including NDP packets, NTDP packets, and handshake packets) to be transmitted in the management VLAN only, through which the management packets are isolated from other packets and network security is improved.
- Enabling the management device and the member devices to communicate with each other in the management VLAN.

Cluster management requires the packets of the management VLAN be permitted on ports connecting the management device and the member/candidate devices. Therefore:

- If the packets of management VLAN are not permitted on a candidate device port connecting to the management device, the candidate device cannot be added to the cluster. In this case, you can enable the packets of the management VLAN to be permitted on the port through the management VLAN auto-negotiation function.
- Packets of the management VLAN can be exchanged between the management device and a member device/candidate device without carrying VLAN tags only when the default VLAN ID of both the two ports connecting the management device and the member/candidate device is the management VLAN. If the VLAN IDs of the both sides are not that of the management VLAN, packets of the management VLAN need to be tagged.

Note

- By default, the management VLAN interface is used as the network management interface.
- There is only one network management interface on a management device; any newly configured network management interface will overwrite the old one.

Tracing a device in a cluster

In practice, you need to implement the following in a cluster sometimes:

- Know whether there is a loop in the cluster
- Locate which port on which switch initiates a network attack
- Determine the port and switch that a MAC address corresponds to
- Locate which switch in the cluster has a fault
- Check whether a link in the cluster and the devices on the link comply with the original plan

In these situations, you can use the **tracemac** command to trace a device in the cluster by specifying a destination MAC address or IP address.

The procedures are as follows:

1) Determine whether the destination MAC address or destination IP address is used to trace a device in the cluster

- If you use the **tracemac** command to trace the device by its MAC address, the switch will query its MAC address table according to the MAC address and VLAN ID in the command to find out the port connected with the downstream switch.
- If you use the **tracemac** command to trace the device by its IP address, the switch will query the corresponding ARP entry of the IP address to find out the corresponding MAC address and VLAN ID, and thus find out the port connected with the downstream switch.

2) After finding out the port connected with the downstream switch, the switch will send a multicast packet with the VLAN ID and specified hops to the port. Upon receiving the packet, the

downstream switch compares its own MAC address with the destination MAC address carried in the multicast packet:

- If the two MAC addresses are the same, the downstream switch sends a response to the switch sending the **tracemac** command, indicating the success of the **tracemac** command.
- If the two MAC addresses are different, the downstream switch will query the port connected with its downstream switch based on the MAC address and VLAN ID, and then forward the packet to its downstream switch. If within the specified hops, a switch with the specified destination MAC address is found, this switch sends a response to the switch sending the **tracemac** command, indicating the success of the **tracemac** command. If no switch with the specified destination MAC address (or IP address) is found, the multicast packet will not be forwarded to the downstream any more.

Note

- If the queried IP address has a corresponding ARP entry, but the MAC address entry corresponding to the IP address does not exist, the trace of the device fails.
- To trace a specific device using the **tracemac** command, make sure that all the devices passed support the **tracemac** function.
- To trace a specific device in a management VLAN using the **tracemac** command, make sure that all the devices passed are within the same management VLAN as the device to be traced.

Cluster Configuration Task List

Before configuring a cluster, you need to determine the roles and functions the switches play. You also need to configure the related functions, preparing for the communication between devices within the cluster.

Complete the following tasks to configure cluster:

Task	Remarks
Configuring the Management Device	Required
Configuring Member Devices	Required
Managing a Cluster through the Management Device	Optional
Configuring the Enhanced Cluster Features	Optional
Configuring the Cluster Synchronization Function	Optional

Configuring the Management Device

Management device configuration task list

Complete the following tasks to configure management device:

Task	Remarks
Enabling NDP globally and on specific ports	Required
Configuring NDP-related parameters	Optional
Enabling NTDP globally and on a specific port	Required
Configuring NTDP-related parameters	Optional
Enabling the cluster function	Required
Configuring cluster parameters	Required
Configuring inside-outside interaction for a cluster	Optional
Configuring the network management interface for a cluster	Optional
Enabling management VLAN synchronization	Optional

Note

To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the Switch 4500 series Ethernet switches provide the following functions, so that a cluster socket is opened only when it is needed:

- Opening UDP port 40000 (used for cluster) only when the cluster function is implemented,
- Closing UDP port 40000 at the same time when the cluster function is closed.

On the management device, the preceding functions are implemented as follows:

- When you create a cluster by using the **build** or **auto-build** command, UDP port 40000 is opened at the same time.
- When you remove a cluster by using the **undo build** or **undo cluster enable** command, UDP port 40000 is closed at the same time.

Enabling NDP globally and on specific ports

Follow these steps to enable NDP globally and on specific ports:

<table>
<tr><th colspan="3">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="3">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="3">Enable NDP globally</td><td>ndp enable</td><td>Required
By default, NDP is enabled globally.</td></tr>
<tr><td rowspan="3">Enable NDP on specified Ethernet ports</td><td colspan="2">In system view</td><td>ndp enable interface port-list</td><td rowspan="3">Use either approach.
By default, NDP is enabled on a port.</td></tr>
<tr><td rowspan="2">In Ethernet port view</td><td>Enter Ethernet port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>Enable NDP on the port</td><td>ndp enable</td></tr>
</table>

Configuring NDP-related parameters

Follow these steps to configure NDP-related parameters:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the holdtime of NDP information	**ndp timer aging** *aging-in-seconds*	Optional By default, the holdtime of NDP information is 180 seconds.
Configure the interval to send NDP packets	**ndp timer hello** *seconds*	Optional By default, the interval to send NDP packets is 60 seconds.

Enabling NTDP globally and on a specific port

Follow these steps to enable NTDP globally and on a specific port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable NTDP globally	**ntdp enable**	Required Enabled by default
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable NTDP on the Ethernet port	**ntdp enable**	Required Enabled by default

Configuring NTDP-related parameters

Follow these steps to configure NTDP-related parameters:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the range to collect topology information	**ntdp hop** *hop-value*	Optional By default, the system collects topology information from the devices within three hops.
Configure the device forward delay of topology collection requests	**ntdp timer hop-delay** *time*	Optional By default, the device forward delay is 200 ms.
Configure the port forward delay of topology collection requests	**ntdp timer port-delay** *time*	Optional By default, the port forward delay is 20 ms.
Configure the interval to collect topology information periodically	**ntdp timer** *interval-in-minutes*	Optional By default, the topology collection interval is one minute.
Quit system view	**quit**	—

To do…	Use the command…	Remarks
Launch topology information collection manually	**ntdp explore**	Optional

Enabling the cluster function

Follow these steps to enable the cluster function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the cluster function globally	**cluster enable**	Required By default, the cluster function is enabled.

Configuring cluster parameters

The establishment of a cluster and the related configuration can be accomplished in manual mode or automatic mode, as described below.

1) Establishing a cluster and configuring cluster parameters in manual mode

Follow these steps to establish a cluster and configure cluster parameters in manual mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify the management VLAN	**management-vlan** *vlan-id*	Required By default, VLAN 1 is used as the management VLAN.
Enter cluster view	**cluster**	—
Configure a IP address pool for the cluster	**ip-pool** *administrator-ip-address* { *ip-mask* | *ip-mask-length* }	Required
Build a cluster	**build** *name*	Required *name*: Cluster name.
Configure a multicast MAC address for the cluster	**cluster-mac** *H-H-H*	Required By default, the cluster multicast MAC address is 0180-C200-000A.
Set the interval for the management device to send multicast packets	**cluster-mac syn-interval** *time-interval*	Optional By default, the interval to send multicast packets is one minutes.
Set the holdtime of member switches	**holdtime** *seconds*	Optional By default, the holdtime is 60 seconds.
Set the interval to send handshake packets	**timer** *interval*	Optional By default, the interval to send handshake packets is 10 seconds.

2) Establish a cluster in automatic mode

Follow these steps to establish a cluster in automatic mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter cluster view	**cluster**	—
Configure the IP address range for the cluster	**ip-pool** *administrator-ip-address* { *ip-mask* | *ip-mask-length* }	Required
Start automatic cluster establishment	**auto-build** [**recover**]	Required Follow prompts to establish a cluster.

Note

- After a cluster is established automatically, ACL 3998 and ACL 3999 will be generated automatically.
- After a cluster is established automatically, ACL 3998 and ACL 3999 can neither be modified nor removed.

Configuring inside-outside interaction for a cluster

Follow these steps to configure inside-outside interaction for a cluster:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter cluster view	**cluster**	Required
Configure a shared FTP server for the cluster	**ftp-server** *ip-address*	Optional By default, the management device acts as the shared FTP server.
Configure a shared TFTP server for the cluster	**tftp-server** *ip-address*	Optional By default, no shared TFTP server is configured.
Configure a shared logging host for the cluster	**logging-host** *ip-address*	Optional By default, no shared logging host is configured.
Configure a shared SNMP host for the cluster	**snmp-host** *ip-address*	Optional By default, no shared SNMP host is configured.

Configuring the network management interface for a cluster

1) Configuration prerequisites

- The cluster switches are properly connected;
- The shared servers are properly connected to the management switch.

2) Configuration procedure

Follow these steps to configure the network management interface for a cluster:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter cluster view	**cluster**	Required
Configure the network management (NM) interface for the cluster	**nm-interface Vlan-interface** *vlan-id*	Required By default, the management VLAN interface is used as the NM interface.

Enabling management VLAN synchronization

By default, VLAN 1 is the management VLAN. To specify another VLAN as the management VLAN for the cluster, you must configure the same management VLAN on all the devices that are about to join the cluster.

By enabling the management VLAN synchronization function on the management device, you can enable the management device to send a management VLAN synchronization packet periodically to the connected devices. After the devices receive the management VLAN synchronization packet, they set their own management VLANs according to the packet. In this way, all devices set the same management VLAN automatically, and thus simplify your configurations.

Follow these steps to enable management VLAN synchronization:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter cluster view	**cluster**	Required
Enable management VLAN synchronization	**management-vlan synchronization enable**	Required Disabled by default.

Configuring Member Devices

Member device configuration task list

Complete the following tasks to configure the member device:

Task	Remarks
Enabling NDP globally and on specific ports	Required
Enabling NTDP globally and on a specific port	Required
Enabling the cluster function	Required
Accessing the shared FTP/TFTP server from a member device	Optional

Note

To reduce the risk of being attacked by malicious users against opened socket and enhance switch security, the Switch 4500 series Ethernet switches provide the following functions, so that a cluster socket is opened only when it is needed:

- Opening UDP port 40000 (used for cluster) only when the cluster function is implemented,
- Closing UDP port 40000 at the same time when the cluster function is closed.

On member devices, the preceding functions are implemented as follows:

- When you execute the **add-member** command on the management device to add a candidate device to a cluster, the candidate device changes to a member device and its UDP port 40000 is opened at the same time.
- When you execute the **auto-build** command on the management device to have the system automatically add candidate devices to a cluster, the candidate devices change to member devices and their UDP port 40000 is opened at the same time.
- When you execute the **administrator-address** command on a device, the device's UDP port 40000 is opened at the same time.
- When you execute the **delete-member** command on the management device to remove a member device from a cluster, the member device's UDP port 40000 is closed at the same time.
- When you execute the **undo build** command on the management device to remove a cluster, UDP port 40000 of all the member devices in the cluster is closed at the same time.
- When you execute the **undo administrator-address** command on a member device, UDP port 40000 of the member device is closed at the same time.

Enabling NDP globally and on specific ports

Follow these steps to enable NDP globally and on specific ports:

<table>
<tr><th colspan="3">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="3">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="3">Enable NDP globally</td><td>ndp enable</td><td>Required</td></tr>
<tr><td rowspan="3">Enable NDP on specified ports</td><td colspan="2">In system view</td><td>ndp enable interface port-list</td><td rowspan="3">Required
Use either approach.</td></tr>
<tr><td rowspan="2">In Ethernet port view</td><td>Enter Ethernet port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>Enable NDP on the port</td><td>ndp enable</td></tr>
</table>

Enabling NTDP globally and on a specific port

Follow these steps to enable NTDP globally and a specific port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable NTDP globally	**ntdp enable**	Required

To do…	Use the command…	Remarks
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable NTDP on the port	**ntdp enable**	Required

Enabling the cluster function

Follow these steps to enable the cluster function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the cluster function globally	**cluster enable**	Optional By default, the cluster function is enabled.

Accessing the shared FTP/TFTP server from a member device

Follow these steps to access the shared FTP/TFTP server from a member device:

To do…	Use the command…	Remarks
Access the shared FTP server of the cluster	**ftp cluster**	Optional Available in user view
Download a file from the shared TFTP server of the cluster	**tftp cluster get** *source-file* [*destination-file*]	Optional Available in user view
Upload a file to the shared TFTP server of the cluster	**tftp cluster put** *source-file* [*destination-file*]	Optional Available in user view

Managing a Cluster through the Management Device

You can manage the member devices through the management device, for example, adding/removing a cluster member, rebooting a member device, logging into a member device, and so on.

Follow these steps to manage a cluster through management device:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter cluster view	**cluster**	—
Add a candidate device to the cluster	**add-member** [*member-number*] **mac-address** *H-H-H* [**password** *password*]	Optional
Remove a member device from the cluster	**delete-member** *member-number*	Optional
Reboot a specified member device	**reboot member** { *member-number* | **mac-address** *H-H-H* } [**eraseflash**]	Optional

To do…	Use the command…	Remarks
Return to system view	**quit**	—
Return to user view	**quit**	—
Switch between management device and member device	**cluster switch-to** { *member-number* | **mac-address** *H-H-H* | **administrator** }	Optional You can use this command switch to the view of a member device and switch back.
Configure the MAC address of the management device	**administrator-address** *mac-address* **name** *name*	Optional By default, a switch does not belong to any cluster.
Trace a device through MAC address or IP address	**tracemac** { **by-mac** *mac-address* **vlan** *vlan-id* | **by-ip** *ip-address* } [**nondp**]	Optional Available in any view

Configuring the Enhanced Cluster Features

Enhanced cluster feature overview

1) Cluster topology management function

After the cluster topology becomes stable, you can use the topology management commands on the cluster administrative device to save the topology of the current cluster as the standard topology and back up the standard topology on the Flash memory of the administrative device.

When errors occur to the cluster topology, you can replace the current topology with the standard cluster topology and restore the administrative device using the backup topology on the Flash memory, so that the devices in the cluster can resume normal operation.

With the **display cluster current-topology** command, the switch can display the topology of the current cluster in a tree structure. The output formats include:

- Display the tree structure three layers above or below the specified node.
- Display the topology between two connected nodes.

Note

The topology information is saved as **topology.top** in the Flash memory to the administrative device. You cannot specify the file name manually.

---

2) Cluster device blacklist function

To ensure stability and security of the cluster, you can use the blacklist to restrict the devices to be added to the cluster. After you add the MAC address of the device that you need to restrict into the cluster blacklist, even if the cluster function is enabled on this device and the device is normally connected to the current cluster, this device cannot join the cluster and participate in the unified management and configuration of the cluster.

Configuring the enhanced cluster features

Complete the following tasks to configure the enhanced cluster feature:

Task	Remarks
Configuring cluster topology management function	Required
Configuring cluster device blacklist	Required

Configuring cluster topology management function

1) Configuration prerequisites

Before configuring the cluster topology management function, make sure that:

- The basic cluster configuration is completed.
- Devices in the cluster work normally.

2) Configuration procedure

Follow these steps to configure cluster topology management function on a management device:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter cluster view	**cluster**	—
Check the current topology and save it as the standard topology.	**topology accept** { **all** [**save-to local-flash**] | **mac-address** *mac-address* | **member-id** *member-id* | **administrator** }	Required
Save the standard topology to the Flash memory of the administrative device	**topology save-to local-flash**	Required
Restore the standard topology from the Flash memory of the administrative device	**topology restore-from local-flash**	Optional
Display the detailed information about a single device	**display ntdp single-device mac-address** *mac-address*	Optional These commands can be executed in any view.
Display the topology of the current cluster	**display cluster current-topology** [**mac-address** *mac-address1* [**to-mac-address** *mac-address2*] | **member-id** *member-id1* [**to-member-id** *member-id2*]]	
Display the information about the base topology of the cluster	**display cluster base-topology** [**mac-address** *mac-address* | **member** *member-id*]	
Display the information about all the devices in the base cluster topology	**display cluster base-members**	

Note

If the management device of a cluster is a slave device in an XRN fabric, the standard topology information is saved only to the local Flash of the master device in the XRN fabric.

Configuring cluster device blacklist

Follow these steps to configure the cluster device blacklist on a management device:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter cluster view	**cluster**	—
Add the MAC address of a specified device to the cluster blacklist	**black-list add-mac** *mac-address*	Optional By default, the cluster blacklist is empty.
Delete the specified MAC address from the cluster blacklist	**black-list delete-mac** *mac-address*	Optional
Delete a device from the cluster add this device to the cluster blacklist	**delete-member** *member-id* [**to-black-list**]	Optional
Displays the information about the devices in the cluster blacklist	**display cluster black-list**	Optional This command can be executed in any view.

Configuring the Cluster Synchronization Function

After a cluster is established, to simplify the access and management to the cluster, you can synchronize the SNMP configurations on the management device and the local user configurations to the member devices of the cluster by configuring the cluster synchronization function.

SNMP configuration synchronization

With this function, you can configure the public SNMP community name, SNMP group, SNMP users and MIB views. These configurations will be synchronized to the member devices of the cluster automatically, which not only simplifies the configurations on the member devices, but also enables the network management station (NMS) to access any member device of the cluster conveniently.

Note

For the SNMP configurations, refer to the *SNMP-RMON Operation* part in this manual.

1) Configuration prerequisites

- NDP and NTDP have been enabled on the management device and member devices, and NDP- and NTDP-related parameters have been configured.
- A cluster is established, and you can manage the member devices through the management device.

2) Configuration procedure

Perform the following operations on the management device to synchronize SNMP configurations:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter cluster view	**cluster**	—
Create a public SNMP community for the cluster	**cluster-snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name*]	Required Not configured by default.
Create a public SNMPv3 group for the cluster	**cluster-snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*]	Required Not configured by default.
Add a public SNMPv3 user to the group	**cluster-snmp-agent usm-user v3** *username groupname* [**authentication-mode** { **md5** | **sha** } *authpassstring* [**privacy-mode** { **des56** *privpassstring* }]]	Required Not configured by default.
Create or update the public MIB view information for the cluster	**cluster-snmp-agent mib-view included** *view-name oid-tree*	Required Not configured by default.

Note

- Perform the above operations on the management device of the cluster.
- Configuring the public SNMP information is equal to executing these configurations on both the management device and the member devices (refer to the SNMP-RMON Operation part in this manual), and these configurations will be saved to the configuration files of the management device and the member devices.
- The public SNMP configurations cannot be synchronized to the devices that are on the cluster blacklist.
- If a member device leaves the cluster, the public SNMP configurations will not be removed.

3) Configuration example

Configure the public SNMP information for the cluster on the management device, including the following:

- The read community name is **read_a**
- The write community name is **write_a**
- The group name is **group_a**

- The MIB view name is **mib_a**, which includes all objects of the subtree **org**
- The SNMPv3 user is **user_a**, which belongs to the group **group_a**.

Create a community with the name of **read_a**, allowing read-only access right using this community name.

```
[test_0.Sysname-cluster] cluster-snmp-agent community read read_a
 Member 2 succeeded in the read-community configuration.
 Member 1 succeeded in the read-community configuration.
 Finish to synchronize the command.
```

Create a community with the name of **write_a**, allowing read and write access right using this community name.

```
[test_0.Sysname-cluster] cluster-snmp-agent community write write_a
 Member 2 succeeded in the write-community configuration.
 Member 1 succeeded in the write-community configuration.
 Finish to synchronize the command.
```

Create an SNMP group **group_a**.

```
[test_0.Sysname-cluster] cluster-snmp-agent group v3 group_a
 Member 2 succeeded in the group configuration.
 Member 1 succeeded in the group configuration.
 Finish to synchronize the command.
```

Create a MIB view **mib_a**, which includes all objects of the subtree **org**.

```
[test_0.Sysname-cluster] cluster-snmp-agent mib-view included mib_a org
 Member 2 succeeded in the mib-view configuration.
 Member 1 succeeded in the mib-view configuration.
 Finish to synchronize the command.
```

Add a user **user_a** to the SNMPv3 group **group_a**.

```
[test_0.Sysname-cluster] cluster-snmp-agent usm-user v3 user_a group_a
 Member 2 succeeded in the usm-user configuration.
 Member 1 succeeded in the usm-user configuration.
 Finish to synchronize the command.
```

After the above configuration, you can see that the public SNMP configurations for the cluster are saved to the management device and member devices by viewing the configuration files.

- Configuration file content on the management device (only the SNMP-related information is displayed)

```
[test_0.Sysname-cluster] display current-configuration
#
cluster
 cluster-snmp-agent community read read_a
 cluster-snmp-agent community write write_a
 cluster-snmp-agent group v3 group_a
 cluster-snmp-agent mib-view included mib_a org
 cluster-snmp-agent usm-user v3 user_a group_a
#
 snmp-agent
 snmp-agent local-engineid 800007DB000FE22405626877
```

```
 snmp-agent community read read_a@cm0
 snmp-agent community write write_a@cm0
 snmp-agent sys-info version all
 snmp-agent group v3 group_a
 snmp-agent mib-view included mib_a org
 snmp-agent usm-user v3 user_a group_a
 undo snmp-agent trap enable standard
```

- Configuration file content on a member device (only the SNMP-related information is displayed)

```
<test_2.Sysname> display current-configuration
#
 snmp-agent
 snmp-agent local-engineid 800007DB000FE224055F6877
 snmp-agent community read read_a@cm2
 snmp-agent community write write_a@cm2
 snmp-agent sys-info version all
 snmp-agent group v3 group_a
 snmp-agent mib-view included mib_a org
 snmp-agent usm-user v3 user_a group_a
```

Local user configuration synchronization

With this function, you can create a public local user for the cluster on the management device, and the username and password will be synchronized to the member devices of the cluster, which is equal to creating this local user on all member devices.

The configured local user is a Telnet user, and you can use the public username and password to manage all member devices through Web.

1) Configuration prerequisites

- NDP and NTDP have been enabled on the management device and member devices, and NDP- and NTDP-related parameters have been configured.
- A cluster is established, and you can manage the member devices through the management device.

2) Configuration procedure

Perform the following operations on the management device to synchronize local user configurations:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter cluster view	**cluster**	—
Create a public local user	**cluster-local-user** *username* **passward { cipher | simple }** *passwardstring*	Required Not configured by default.

Note

- Perform the above operations on the management device of the cluster.
- Creating a public local user is equal to executing these configurations on both the management device and the member devices (refer to the AAA Operation part in this manual), and these configurations will be saved to the configuration files of the management device and the member devices.
- The public local user configurations cannot be synchronized to the devices that are on the cluster blacklist.
- If a member device leaves the cluster, the public local user configurations will not be removed.

Displaying and Maintaining Cluster Configuration

To do…	Use the command…	Remarks
Display all NDP configuration and running information (including the interval to send NDP packets, the holdtime, and all neighbors discovered)	**display ndp**	Available in any view.
Display NDP configuration and running information on specified ports (including the neighbors discovered by NDP on the ports)	**display ndp interface** *port-list*	
Display global NTDP information	**display ntdp**	
Display device information collected by NTDP	**display ntdp device-list** [**verbose**]	
Display status and statistics information about the cluster	**display cluster**	
Display information about the candidate devices of the cluster	**display cluster candidates** [**mac-address** *H-H-H* | **verbose**]	
Display information about the member devices of the cluster	**display cluster members** [*member-number* | **verbose**]	
Clear the statistics on NDP ports	**reset ndp statistics** [**interface** *port-list*]	Available in user view.

Note

When you display the cluster topology information, the devices attached to the switch that is listed in the backlist will not be displayed.

Cluster Configuration Examples

Basic Cluster Configuration Example

Network requirements

Three switches compose a cluster, where:

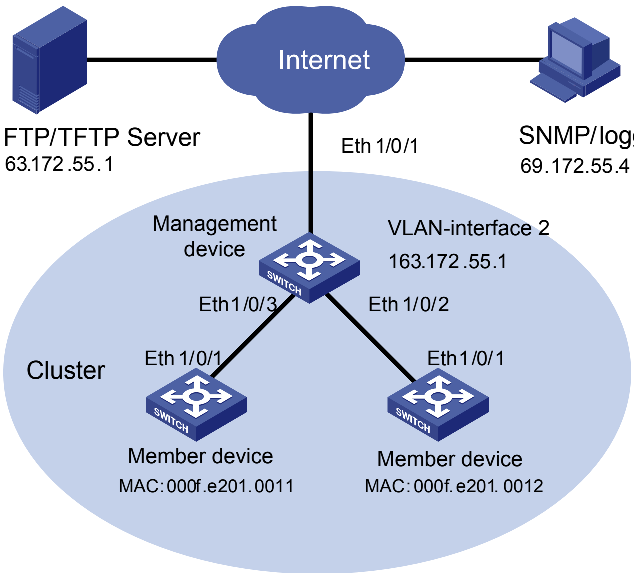
- A Switch 4500 series switch serves as the management device.
- The rest are member devices.

Serving as the management device, the Switch 4500 switch manages the two member devices. The configuration for the cluster is as follows:

- The two member devices connect to the management device through Ethernet 1/0/2 and Ethernet 1/0/3.
- The management device connects to the Internet through Ethernet 1/0/1.
- Ethernet 1/0/1 belongs to VLAN 2, whose interface IP address is 163.172.55.1.
- All the devices in the cluster share the same FTP server and TFTP server.
- The FTP server and TFTP server use the same IP address: 63.172.55.1.
- The NMS and logging host use the same IP address: 69.172.55.4.

Network diagram

Figure 1-4 Network diagram for HGMP cluster configuration



Configuration procedure

1) Configure the member devices (taking one member as an example)

Enable NDP globally and on Ethernet 1/0/1.

```
<Sysname> system-view
[Sysname] ndp enable
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] ndp enable
[Sysname-Ethernet1/0/1] quit
```

Enable NTDP globally and on Ethernet 1/0/1.

```
[Sysname] ntdp enable
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] ntdp enable
[Sysname-Ethernet1/0/1] quit
```

Enable the cluster function.

```
[Sysname] cluster enable
```

2) Configure the management device

Add port Ethernet 1/0/1 to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port Ethernet 1/0/1
[Sysname-vlan2] quit
```

Configure the IP address of VLAN-interface 2 as 163.172.55.1.

```
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] ip address 163.172.55.1 255.255.255.0
[Sysname-Vlan-interface2] quit
```

Disable NDP on the uplink port Ethernet 1/0/1.

```
[Sysname] ndp enable
[Sysname] undo ndp enable interface Ethernet 1/0/1
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] undo ntdp enable
[Sysname-Ethernet1/0/1] quit
```

Enable NDP on Ethernet 1/0/2 and Ethernet 1/0/3.

```
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] ndp enable
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] ndp enable
[Sysname-Ethernet1/0/3] quit
```

Set the hold time of NDP information to 200 seconds.

```
[Sysname] ndp timer aging 200
```

Set the interval between sending NDP packets to 70 seconds.

```
[Sysname] ndp timer hello 70
```

Enable NTDP globally and on Ethernet 1/0/2 and Ethernet 1/0/3.

```
[Sysname] ntdp enable
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] ntdp enable
[Sysname-Ethernet1/0/2] quit
[Sysname] interface Ethernet 1/0/3
[Sysname-Ethernet1/0/3] ntdp enable
[Sysname-Ethernet1/0/3] quit
```

Set the topology collection range to 2 hops.

```
[Sysname] ntdp hop 2
```

Set the delay for a member device to forward topology collection requests to 150 ms.

```
[Sysname] ntdp timer hop-delay 150
```

Set the delay for a member device port to forward topology collection requests to 15 ms.

```
[Sysname] ntdp timer port-delay 15
```

Set the interval between collecting topology information to 3 minutes.

```
[Sysname] ntdp timer 3
```

Enable the cluster function.

```
[Sysname] cluster enable
```

Enter cluster view.

```
[Sysname] cluster
[Sysname-cluster]
```

Configure a private IP address pool for the cluster. The IP address pool contains six IP addresses, starting from 172.16.0.1.

```
[Sysname-cluster] ip-pool 172.16.0.1 255.255.255.248
```

Name and build the cluster.

```
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster]
```

Add the attached two switches to the cluster.

```
[aaa_0.Sysname-cluster] add-member 1 mac-address 000f-e201-0011
[aaa_0.Sysname-cluster] add-member 17 mac-address 000f-e201-0012
```

Set the holdtime of member device information to 100 seconds.

```
[aaa_0.Sysname-cluster] holdtime 100
```

Set the interval between sending handshake packets to 10 seconds.

```
[aaa_0.Sysname-cluster] timer 10
```

Configure VLAN-interface 2 as the network management interface.

```
[aaa_0.Sysname-cluster] nm-interface Vlan-interface 2
```

Configure the shared FTP server, TFTP server, logging host and SNMP host for the cluster.

```
[aaa_0.Sysname-cluster] ftp-server 63.172.55.1
[aaa_0.Sysname-cluster] tftp-server 63.172.55.1
[aaa_0.Sysname-cluster] logging-host 69.172.55.4
[aaa_0.Sysname-cluster] snmp-host 69.172.55.4
```

3) Perform the following operations on the member devices (taking one member as an example)

After adding the devices attached to the management device to the cluster, perform the following operations on a member device.

Connect the member device to the remote shared FTP server of the cluster.

```
<aaa_1.Sysname> ftp cluster
```

Download the file named **aaa.txt** from the shared TFTP server of the cluster to the member device.

```
<aaa_1.Sysname> tftp cluster get aaa.txt
```

Upload the file named **bbb.txt** from the member device to the shared TFTP server of the cluster.

```
<aaa_1.Sysname> tftp cluster put bbb.txt
```

Note

- After completing the above configuration, you can execute the **cluster switch-to** { *member-number* | **mac-address** *H-H-H* } command on the management device to switch to member device view to maintain and manage a member device. After that, you can execute the **cluster switch-to administrator** command to return to management device view.
- In addition, you can execute the **reboot member** { *member-number* | **mac-address** *H-H-H* } [**eraseflash**] command on the management device to reboot a member device. For detailed information about these operations, refer to the preceding description in this chapter.
- After the above configuration, you can receive logs and SNMP trap messages of all cluster members on the NMS.

Network Management Interface Configuration Example

Network requirements

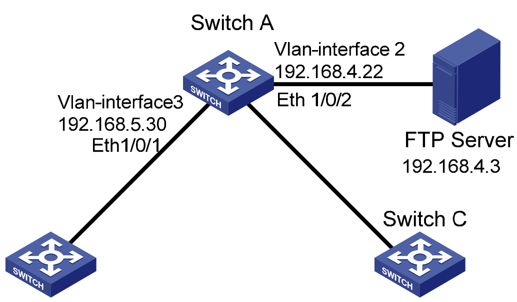
- Configure VLAN-interface 2 as the network management interface of the switch;
- Configure VLAN 3 as the management VLAN;
- The IP address of the FTP server is 192.168.4.3;
- Switch A operates as the management switch;
- Switch B and Switch C are member switches.

Table 1-2 Connection information of the management switch

VLAN	IP address	Connection port
VLAN 3 (connected to Switch B)	192.168.5.30/24	Ethernet 1/0/1
VLAN 2 (connected to FTP server)	192.168.4.22/24	Ethernet 1/0/2

Network diagram

Figure 1-5 Network diagram for network management interface configuration



Configuration procedure

Enter system view and configure VLAN 3 as the management VLAN.

```
<Sysname> system-view
[Sysname] management-vlan 3
```

Add Ethernet 1/0/1 to VLAN 3.

```
[Sysname] vlan 3
[Sysname-vlan3] port Ethernet 1/0/1
[Sysname-vlan3] quit
```

Set the IP address of VLAN-interface 3 to 192.168.5.30.

```
[Sysname] interface Vlan-interface 3
[Sysname-Vlan-interface3] ip address 192.168.5.30 255.255.255.0
[Sysname-Vlan-interface3] quit
```

Add Ethernet 1/0/2 to VLAN 2.

```
[Sysname] vlan 2
[Sysname-vlan2] port Ethernet 1/0/2
[Sysname-vlan2] quit
```

Set the IP address of VLAN-interface 2 to 192.168.4.22.

```
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] ip address 192.168.4.22 255.255.255.0
[Sysname-Vlan-interface2] quit
```

Enable the cluster function.

```
[Sysname] cluster enable
```

Enter cluster view.

```
[Sysname] cluster
[Sysname-cluster]
```

Configure a private IP address pool for the cluster. The IP address pool contains 30 IP addresses, starting from 192.168.5.1.

```
[Sysname-cluster] ip-pool 192.168.5.1 255.255.255.224
```

Name and build the cluster.

```
[Sysname-cluster] build aaa
[aaa_0.Sysname-cluster]
```

Configure VLAN-interface 2 as the network management interface.

```
[aaa_0.Sysname] cluster
[aaa_0.Sysname-cluster] nm-interface Vlan-interface 2
```

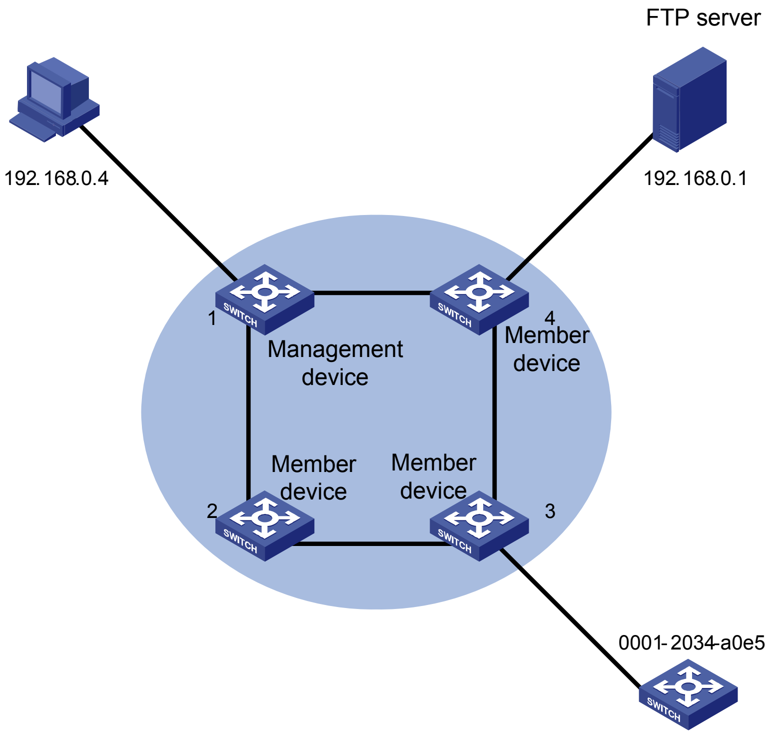
Enhanced Cluster Feature Configuration Example

Network requirements

- The cluster operates properly.
- Add the device with the MAC address 0001-2034-a0e5 to the cluster blacklist, that is, prevent the device from being managed and maintained by the cluster.
- Save the current cluster topology as the base topology and save it in the flash of the local management device in the cluster.

Network diagram

Figure 1-6 Network diagram for the enhanced cluster feature configuration



Configuration procedure

Enter cluster view.

```
<aaa_0.Sysname> system-view
[aaa_0.Sysname] cluster
```

Add the MAC address 0001-2034-a0e5 to the cluster blacklist.

```
[aaa_0.Sysname-cluster] black-list add-mac 0001-2034-a0e5
```

Backup the current topology.

```
[aaa_0.Sysname-cluster] topology accept all save-to local-flash
```

Table of Contents

1 PoE Configuration

When configuring PoE, go to these sections for information you are interested in:

- PoE Overview
- PoE Configuration
- PoE Configuration Example

PoE Overview

Introduction to PoE

Power over Ethernet (PoE)-enabled devices use twisted pairs through electrical ports to supply power to the remote powered devices (PD) in the network and implement power supply and data transmission simultaneously.

Advantages of PoE

- Reliability: The centralized power supply provides backup convenience, unified management, and safety.
- Easy connection: Network terminals only require an Ethernet cable, but no external power supply.
- Standard: PoE conforms to the 802.3af standard and uses a globally uniform power interfaces;
- Bright application prospect: PoE can be applied to IP phones, wireless access points (APs), chargers for portable devices, card readers, network cameras, and data collection system.

PoE components

PoE consists of three components: power sourcing equipment (PSE), PD, and power interface (PI).

- PSE: PSE is comprised of the power and the PSE functional module. It can implement PD detection, PD power information collection, PoE, power supply monitoring, and power-off for devices.
- PD: PDs receive power from the PSE. PDs include standard PDs and nonstandard PDs. Standard PDs conform to the 802.3af standard, including IP phones, Wireless APs, network cameras and so on.
- PI: PIs are RJ45 interfaces which connect PSE/PDs to network cables.

PoE Features Supported by Switch 4500

PoE-capable 4500 switches include:

- Switch 4500 PWR 26-Port
- Switch 4500 PWR 50-Port

A PoE-capable Switch 4500 has the following features:

- As the PSE, it supports the IEEE802.3af standard. It can also supply power to the PDs that do not support the 802.3af standard.
- It can deliver data and current simultaneously through data wires (1,2,3,and 6) of category-3/5 twisted pairs.

- Through the fixed 24/48 Ethernet electrical ports, it can supply power to up to 24/48 remote Ethernet switches with a maximum distance of 100 m (328 feet).
- Each Ethernet electrical port can supply at most a power of 15,400 mW to a PD.
- When AC power input is adopted for the switch, the maximum total power that can be provided is 300 W. The switch can determine whether to supply power to the next remote PD it detects depending on its available power.
- When DC power input is adopted for the switch, it is capable of supplying full power to all of the 24/48 ports, that is, 15,400 mW for each port, and the total power is 369.6 W/739.2 W.
- The PSE processing software on the switch can be upgraded online.
- The switch provides statistics about power supplying on each port and the whole equipment, which you can query through the **display** command.
- The switch provides two modes (**auto** and **manual**) to manage the power feeding to ports in the case of PSE power overload.
- The switch provides over-temperature protection mechanism. Using this mechanism, the switch disables the PoE feature on all ports when its internal temperature exceeds 65°C (149°F) for self-protection, and restores the PoE feature on all its ports when the temperature drops below 60°C (140°F).
- The switch supports the PoE profile feature, that is, different PoE policies can be set for different user groups. These PoE policies are each saved in the corresponding PoE profile and applied to ports of the user groups.

Note

- When you use the PoE-capable Switch 4500 to supply power, the PDs need no external power supply.
- If a remote PD has an external power supply, the PoE-capable Switch 4500 and the external power supply will backup each other for the PD.
- Only the 100 Mbps Ethernet electrical ports of the PoE-capable Switch 4500 support the PoE feature.

PoE Configuration

PoE Configuration Task List

Complete the following tasks to configure PoE configuration:

Task	Remarks
Enabling the PoE Feature on a Port	Required
Setting the Maximum Output Power on a Port	Optional
Setting PoE Management Mode and PoE Priority of a Port	Optional
Setting the PoE Mode on a Port	Optional
Configuring a PD Disconnection Detection Mode	Optional
Configuring PoE Over-Temperature Protection on the Switch	Optional

Task	Remarks
Upgrading the PSE Processing Software Online	Optional
Upgrading the PSE Processing Software of Fabric Switches Online	Optional
Displaying PoE Configuration	Optional

Enabling the PoE Feature on a Port

Follow these steps to enable the PoE feature on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the PoE feature on a port	**poe enable**	Required

Caution

- By default, the PoE function on a port is enabled by the default configuration file (config.def) when the device is delivered.
- If you delete the default configuration file without specifying another one, the PoE function on a port will be disabled after you restart the device.

Setting the Maximum Output Power on a Port

The maximum power that can be supplied by each Ethernet electrical port of a PoE-capable Switch 4500 to its PD is 15,400 mW. In practice, you can set the maximum power on a port depending on the actual power of the PD, in the range of 1,000 to 15,400 mW and in the granularity of 100 mW.

Follow these steps to set the maximum output power on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the maximum output power on the port	**poe max-power** *max-power*	Required 15,400 mW by default.

Setting PoE Management Mode and PoE Priority of a Port

When a switch is close to its full load in supplying power, you can adjust the power supply of the switch through the cooperation of the PoE management mode and the port PoE priority settings. Switch 4500 supports two PoE management modes, auto and manual. The auto mode is adopted by default.

- **auto**: When the switch is close to its full load in supplying power, it will first supply power to the PDs that are connected to the ports with critical priority, and then supply power to the PDs that are connected to the ports with high priority. For example: Port A has the priority of critical. When the switch PoE is close to its full load and a new PD is now added to port A, the switch will power down the PD connected to the port with the lowest priority and turn to supply power to this new PD. If more than one port has the same lowest priority, the switch will power down the PD connected to the port with larger port number.
- **manual**: When the switch is close to its full load in supplying power, it will not make change to its original power supply status based on its priority when a new PD is added. For example: Port A has the priority critical. When the switch PoE is close to its full load and a new PD is now added to port A, the switch just gives a prompt that a new PD is added and will not supply power to this new PD.

After the PoE feature is enabled on the port, perform the following configuration to set the PoE management mode and PoE priority of a port.

Follow these steps to set the PoE management mode and PoE priority of a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the PoE management mode for the switch	**poe power-management { auto | manual }**	Required **auto** by default.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Se the PoE priority of a port	**poe priority** { **critical** | **high** | **low** }	Required **low** by default.

Setting the PoE Mode on a Port

PoE mode of a port falls into two types, signal mode and spare mode.

- Signal mode: DC power is carried over the data pairs (1,2,3,and 6) of category-3/5 twisted pairs.
- Spare mode: DC power is carried over the spare pairs (4,5,7,and 8) of category-3/5 twisted pairs.

Currently, Switch 4500 does not support the spare mode.

After the PoE feature is enabled on the port, perform the following configuration to set the PoE mode on a port.

Follow these steps to set the PoE mode on a port:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the PoE mode on the port to signal	**poe mode signal**	Optional **signal** by default.

Configuring the PD Compatibility Detection Function

After the PD compatibility detection function is enabled, the switch can detect the PDs that do not conform to the 802.3af standard and supply power to them.

After the PoE feature is enabled, perform the following configuration to enable the PD compatibility detection function.

Follow these steps to configure the PD compatibility detection function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the PD compatibility detection function	**poe legacy enable**	Required Disabled by default.

Configuring a PD Disconnection Detection Mode

To detect the PD connection with PSE, PoE provides two detection modes: AC detection and DC detection. The AC detection mode is energy saving relative to the DC detection mode.

Follow these steps to configure a PD disconnection detection mode

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a PD disconnection detection mode	**poe disconnect** { **ac** | **dc** }	Optional The default PD disconnection detection mode is AC.

Caution

If you adjust the PD disconnection detection mode when the switch is running, the connected PDs will be powered off. Therefore, be cautious to do so.

Configuring PoE Over-Temperature Protection on the Switch

If this function is enabled, the switch disables the PoE feature on all ports when its internal temperature exceeds 65°C (149°F) for self-protection, and restores the PoE feature settings on all its ports when the temperature drops below 60°C (140°F).

Follow these steps to configure PoE over-temperature protection on the switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable PoE over-temperature protection on the switch	**poe temperature-protection enable**	Optional Enabled by default.

Note

- When the internal temperature of the switch decreases from X (X>65°C, or X>149°F) to Y (60°C≤Y<65°C, or 140°F≤Y<149°F), the switch still keeps the PoE function disabled on all the ports.
- When the internal temperature of the switch increases from X (X<60°C, or X<140°F) to Y (60°C<Y≤65°C, or 140°F<Y≤149°F), the switch still keeps the PoE function enabled on all the ports.

Upgrading the PSE Processing Software Online

The online upgrading of PSE processing software can update the processing software or repair the software if it is damaged. Before performing the following configuration, download the PSE processing software to the Flash of the switch.

Follow these steps to upgrade PSE processing software online:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Upgrade the PSE processing software online	**poe update** { **refresh** | **full** } *filename*	Required The specified PSE processing software is a file with the extension .s19.

Note

- In the case that the PSE processing software is damaged (that is, no **PoE** command can be executed successfully), use the **full** update mode to upgrade and thus restore the software.
- The **refresh** update mode is to upgrade the original processing software in the PSE through refreshing the software, while the **full** update mode is to delete the original processing software in PSE completely and then reload the software.
- Generally, the **refresh** update mode is used to upgrade the PSE processing software.
- When the online upgrading procedure is interrupted for some unexpected reason (for example, the device restarts due to some errors), if the upgrade in **full** mode fails after restart, you must upgrade in **full** mode after power-off and restart of the device, and then restart the device manually. In this way, the former PoE configuration is restored.

Upgrading the PSE Processing Software of Fabric Switches Online

You can update or repair the damaged PSE processing software through upgrading it.

By executing the following command on any device in the fabric, you can upgrade the PSE processing software of all devices in the fabric by using the specified PSE processing software. For details of fabric, see the XRN Fabric part of this manual.

Follow these steps to upgrade the PSE processing software online:

To do…	Use the command…	Remarks
Upgrade the PSE processing software of the fabric switch online	**update fabric** { *file-url* | *device-name file-url* }	Optional

Displaying PoE Configuration

To do…	Use the command…	Remarks
Display the current PD disconnection detection mode of the switch	**display poe disconnect**	Available in any view
Display the PoE status of a specific port or all ports of the switch	**display poe interface** [*interface-type interface-number*]	
Display the PoE power information of a specific port or all ports of the switch	**display poe interface power** [*interface-type interface-number*]	
Display the PSE parameters	**display poe powersupply**	
Display the status (enabled/disabled) of the PoE over-temperature protection feature on the switch	**display poe temperature-protection**	

PoE Configuration Example

PoE Configuration Example

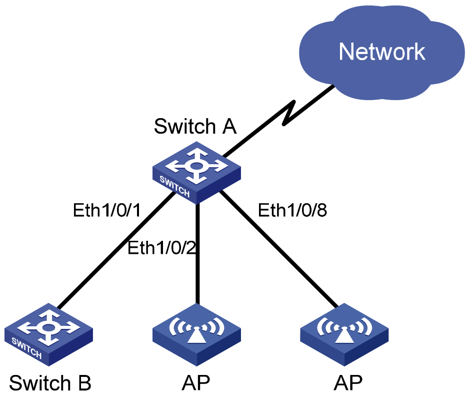
Network requirements

Switch A is a Switch 4500 supporting PoE, Switch B can be PoE powered.

- The Ethernet 1/0/1 and Ethernet 1/0/2 ports of Switch A are connected to Switch B and an AP respectively; the Ethernet 1/0/8 port is intended to be connected with an important AP.
- The PSE processing software of Switch A is first upgraded online. The remotely accessed PDs are powered by Switch A.
- The power consumption of the accessed AP is 2,500 mW, and the maximum power consumption of Switch B is 12,000 mW.
- It is required to guarantee the power feeding to the PDs connected to the Ethernet 1/0/8 port even when Switch A is under full load.

Network diagram

Figure 1-1 Network diagram for PoE



Configuration procedure

Upgrade the PSE processing software online.

```
<SwitchA> system-view
[SwitchA] poe update refresh 0290_021.s19
```

Enable the PoE feature on Ethernet 1/0/1, and set the PoE maximum output power of Ethernet 1/0/1 to 12,000 mW.

```
[SwitchA] interface Ethernet 1/0/1
[SwitchA-Ethernet1/0/1] poe enable
[SwitchA-Ethernet1/0/1] poe max-power 12000
[SwitchA-Ethernet1/0/1] quit
```

Enable the PoE feature on Ethernet 1/0/2, and set the PoE maximum output power of Ethernet 1/0/2 to 2500 mW.

```
[SwitchA] interface Ethernet 1/0/2
[SwitchA-Ethernet1/0/2] poe enable
[SwitchA-Ethernet1/0/2] poe max-power 2500
[SwitchA-Ethernet1/0/2] quit
```

Enable the PoE feature on Ethernet 1/0/8, and set the PoE priority of Ethernet 1/0/8 to critical.

```
[SwitchA] interface Ethernet 1/0/8
[SwitchA-Ethernet1/0/8] poe enable
[SwitchA-Ethernet1/0/8] poe priority critical
[SwitchA-Ethernet1/0/8] quit
```

Set the PoE management mode on the switch to auto (it is the default mode, so this step can be omitted).

```
[SwitchA] poe power-management auto
```

Enable the PD compatibility detect of the switch to allow the switch to supply power to the devices noncompliant with the 802.3af standard.

```
[SwitchA] poe legacy enable
```

2 PoE Profile Configuration

When configuring PoE profile, go to these sections for information you are interested in:

- Introduction to PoE Profile
- PoE Profile Configuration
- Displaying PoE Profile Configuration
- PoE Profile Configuration Example

Introduction to PoE Profile

On a large-sized network or a network with mobile users, to help network administrators to monitor the PoE features of the switch, Switch 4500 provides the PoE profile features. A PoE profile is a set of PoE configurations, including multiple PoE features.

Features of PoE profile:

- Various PoE profiles can be created. PoE policy configurations applicable to different user groups are stored in the corresponding PoE profiles. These PoE profiles can be applied to the ports used by the corresponding user groups.
- When users connect a PD to a PoE-profile-enabled port, the PoE configurations in the PoE profile will be enabled on the port.

PoE Profile Configuration

Configuring PoE Profile

Follow these steps to configure PoE profile:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Create a PoE profile and enter PoE profile view	**poe-profile** *profilename*	Required If the PoE file is created, you will enter PoE profile view directly through the command.

<table>
<tr><th colspan="3">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td rowspan="4">Configure the relevant features in PoE profile</td><td colspan="2">Enable the PoE feature on a port</td><td>poe enable</td><td>Required
Disabled by default.</td></tr>
<tr><td colspan="2">Configure PoE mode for Ethernet ports</td><td>poe mode { signal | spare }</td><td>Optional
signal by default.</td></tr>
<tr><td colspan="2">Configure the PoE priority for Ethernet ports</td><td>poe priority { critical | high | low }</td><td>Optional
low by default.</td></tr>
<tr><td colspan="2">Configure the maximum power for Ethernet ports</td><td>poe max-power max-power</td><td>Optional
15,400 mW by default.</td></tr>
<tr><td colspan="3">Quit system view</td><td>quit</td><td>—</td></tr>
<tr><td rowspan="3">Apply the existing PoE profile to the specified Ethernet port</td><td colspan="2">In system view</td><td>apply poe-profile profile-name interface interface-type interface-number [to interface-type interface-number]</td><td rowspan="3">Use either approach.</td></tr>
<tr><td rowspan="2">In Ethernet port view</td><td>Enter Ethernet port view</td><td>interface interface-type interface-number</td></tr>
<tr><td>Apply the existing PoE profile to the port</td><td>apply poe-profile profile-name</td></tr>
</table>

Note the following during the configuration:

1) When the apply poe-profile command is used to apply a PoE profile to a port, some PoE features in the PoE profile can be applied successfully while some cannot. PoE profiles are applied to Switch 4500 according to the following rules:

- When the **apply poe-profile** command is used to apply a PoE profile to a port, the PoE profile is applied successfully only if one PoE feature in the PoE profile is applied properly. When the **display current-configuration** command is used for query, it is displayed that the PoE profile is applied properly to the port.
- If one or more features in the PoE profile are not applied properly on a port, the switch will prompt explicitly which PoE features in the PoE profile are not applied properly on which ports.
- The **display current-configuration** command can be used to query which PoE profile is applied to a port. However, the command cannot be used to query which PoE features in a PoE profiles are applied successfully.

2) PoE profile configuration is a global configuration, and applies synchronously in the Expandable Resilient Networking (XRN) system.

3) Combination of Unit creates a new Fabric. In the newly created Fabric, the PoE profile configuration of the Unit with the smallest Unit ID number will become the PoE profile configuration for the Fabric currently in use.

4) Split of Fabric results in many new Fabrics. In each newly created Fabric, the PoE profile configuration of each Unit remains the same as it was before the split.

Displaying PoE Profile Configuration

To do…	Use the command…	Remarks
Display the detailed information about the PoE profiles created on the switch	**display poe-profile** { **all-profile** | **interface** *interface-type interface-number* | **name** *profile-name* }	Available in any view

PoE Profile Configuration Example

PoE Profile Application Example

Network requirements

Switch A is a Switch 4500 supporting PoE.

Ethernet 1/0/1 through Ethernet 1/0/10 of Switch A are used by users of group A, who have the following requirements:

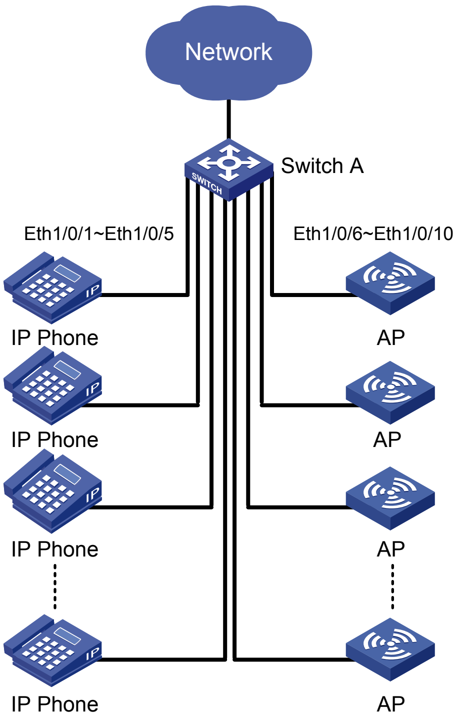
- The PoE function can be enabled on all ports in use.
- Signal mode is used to supply power.
- The PoE priority for Ethernet 1/0/1 through Ethernet 1/0/5 is Critical, whereas the PoE priority for Ethernet 1/0/6 through Ethernet 1/0/10 is High.
- The maximum power for Ethernet 1/0/1 through Ethernet 1/0/5 ports is 3000 mW, whereas the maximum power for Ethernet 1/0/6 through Ethernet 1/0/10 is 15400 mW.

Based on the above requirements, two PoE profiles are made for users of group A.

- Apply PoE profile 1 for Ethernet 1/0/1 through Ethernet 1/0/5;
- Apply PoE profile 2 for Ethernet 1/0/6 through Ethernet 1/0/10.

Network diagram

Figure 2-1 PoE profile application



Configuration procedure

Create Profile 1, and enter PoE profile view.

```
<SwitchA> system-view
[SwitchA] poe-profile Profile1
```

In Profile 1, add the PoE policy configuration applicable to Ethernet 1/0/1 through Ethernet 1/0/5 ports for users of group A.

```
[SwitchA-poe-profile-Profile1] poe enable
[SwitchA-poe-profile-Profile1] poe mode signal
[SwitchA-poe-profile-Profile1] poe priority critical
[SwitchA-poe-profile-Profile1] poe max-power 3000
[SwitchA-poe-profile-Profile1] quit
```

Display detailed configuration information for Profile1.

```
[SwitchA] display poe-profile name Profile1
Poe-profile: Profile1, 3 action
poe enable
poe max-power 3000
poe priority critical
```

Create Profile 2, and enter PoE profile view.

```
[SwitchA] poe-profile Profile2
```

In Profile 2, add the PoE policy configuration applicable to Ethernet 1/0/6 through Ethernet 1/0/10 ports for users of group A.

```
[SwitchA-poe-profile-Profile2] poe enable
```

```
[SwitchA-poe-profile-Profile2] poe mode signal
[SwitchA-poe-profile-Profile2] poe priority high
[SwitchA-poe-profile-Profile2] poe max-power 15400
[SwitchA-poe-profile-Profile2] quit
```

Display detailed configuration information for Profile2.

```
[SwitchA] display poe-profile name Profile2
Poe-profile: Profile2, 2 action
poe enable
poe priority high
```

Apply the configured Profile 1 to Ethernet 1/0/1 through Ethernet 1/0/5 ports.

```
[SwitchA] apply poe-profile Profile1 interface Ethernet1/0/1 to Ethernet1/0/5
```

Apply the configured Profile 2 to Ethernet 1/0/6 through Ethernet 1/0/10 ports.

```
[SwitchA] apply poe-profile Profile2 interface Ethernet1/0/6 to Ethernet1/0/10
```

Table of Contents

1 UDP Helper Configuration

When configuring UDP helper, go to these sections for information you are interested in:

Introduction to UDP Helper

Sometimes, a host needs to forward broadcasts to obtain network configuration information or request the names of other devices on the network. However, if the server or the device to be requested is located in another broadcast domain, the host cannot obtain such information through broadcast.

To solve this problem, S4500 series Ethernet switches provide the UDP Helper function to relay specified UDP packets. In other words, UDP Helper functions as a relay agent that converts UDP broadcast packets into unicast packets and forwards them to a specified destination server.

With UDP Helper enabled, the device decides whether to forward a received UDP broadcast packet according to the UDP destination port number of the packet.

- If the destination port number of the packet matches the one pre-configured on the device, the device modifies the destination IP address in the IP header and then sends the packet to the specified destination server.
- Otherwise, the device sends the packet to the upper layer protocol for processing.

Note

Relay forwarding of BOOTP/DHCP broadcast packets is implemented by the DHCP relay function using UDP ports 67 and 68, so these two ports cannot be configured as UDP Helper relay ports.

By default, with UDP Helper enabled, the device forwards broadcast packets with the six UDP destination port numbers listed in Table 1-1.

Table 1-1 List of default UDP ports

Protocol	UDP port number
DNS (Domain Name System)	53
NetBIOS-DS (NetBIOS Datagram Service)	138
NetBIOS-NS (NetBIOS Name Service)	137
TACACS (Terminal Access Controller Access Control System)	49
TFTP (Trivial File Transfer Protocol)	69

Protocol	UDP port number
Time Service	37

Configuring UDP Helper

Follow these steps to configure UDP Helper:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable UDP Helper	**udp-helper enable**	Required Disabled by default.
Specify a UDP port number	**udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }	Optional By default, the device enabled with UDP Helper forwards the broadcast packets containing any of the six port numbers 53, 138, 137, 49, 69 and 37.
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Specify the destination server to which the UDP packets are to be forwarded	**udp-helper server** *ip-address*	Required No destination server is specified by default.

Note

- You need to enable UDP Helper before specifying any UDP port to match UDP broadcasts; otherwise, the configuration fails. When the UDP helper function is disabled, all configured UDP ports are disabled, including the default ports.
- The **dns**, **netbios-ds**, **netbios-ns**, **tacacs**, **tftp**, and **time** keywords correspond to the six default ports. You can configure the default ports by specifying port numbers or the corresponding parameters. For example, **udp-helper port** 53 and **udp-helper port dns** specify the same port.
- You can specify up to 20 destination server addresses on a VLAN interface.
- If UDP Helper is enabled after a destination server is configured for a VLAN interface, the broadcasts from interfaces belonging to the VLAN and having a matching UDP port will be unicast to the destination server.

Displaying and Maintaining UDP Helper

To do…	Use the command…	Remarks
Display the UDP broadcast relay forwarding information of a specified VLAN interface on the switch	**display udp-helper server** [**interface vlan-interface** *vlan-id*]	Available in any view

To do…	Use the command…	Remarks
Clear statistics about packets forwarded by UDP Helper	**reset udp-helper packet**	Available in user view

UDP Helper Configuration Example

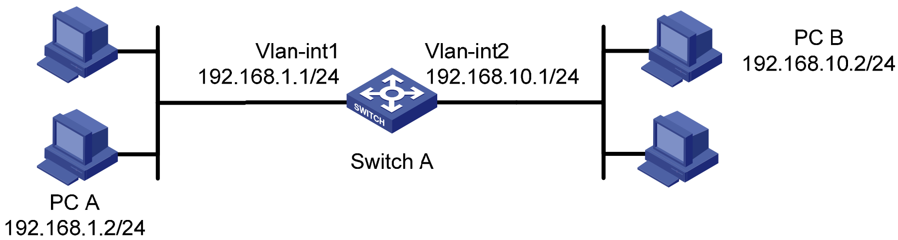
Cross-Network Computer Search Through UDP Helper

Network requirements

PC A resides on network segment 192.168.1.0/24 and PC B on 192.168.10.0/24; they are connected through Switch A and are routable to each other. It is required to configure UDP Helper on the switch, so that PC A can find PC B through computer search. (Broadcasts with UDP port 137 are used for searching.)

Network diagram

Figure 1-1 Network diagram for UDP Helper configuration



Configuration procedure

Enable UDP Helper on Switch A.

```
<SwitchA> system-view
[SwitchA] udp-helper enable
```

Configure the switch to forward broadcasts containing the destination UDP port number 137. (By default, the device enabled with UDP Helper forwards the broadcasts containing the destination UDP port number 137.)

```
[SwitchA] udp-helper port 137
```

Specify the destination server IP address on Vlan-interface 1.

```
[SwitchA] interface Vlan-interface 1
[SwitchA-Vlan-interface1] udp-helper server 192.168.10.2
```

Table of Contents

1 SNMP Configuration

When configuring SNMP, go to these sections for information you are interested in:

SNMP Overview

The Simple Network Management Protocol (SNMP) is used for ensuring the transmission of the management information between any two network nodes. In this way, network administrators can easily retrieve and modify the information about any node on the network. In the meantime, they can locate faults promptly and implement the fault diagnosis, capacity planning and report generating.

As SNMP adopts the polling mechanism and provides basic function set, it is suitable for small-sized networks with fast-speed and low-cost. SNMP is based on User Datagram Protocol (UDP) and is thus widely supported by many products.

SNMP Operation Mechanism

SNMP is implemented by two components, namely, network management station (NMS) and agent.

- An NMS can be a workstation running client program. At present, the commonly used network management platforms include QuidView, Sun NetManager, IBM NetView, and so on.
- Agent is server-side software running on network devices (such as switches).

An NMS can send GetRequest, GetNextRequest and SetRequest messages to the agents. Upon receiving the requests from the NMS, an agent performs Read or Write operation on the managed object (MIB, Management Information Base) according to the message types, generates the corresponding Response packets and returns them to the NMS.

When a network device operates improperly or changes to other state, the agent on it can also send traps on its own initiative to the NMS to report the events.

SNMP Versions

Currently, SNMP agent on a switch supports SNMPv3, and is compatible with SNMPv1 and SNMPv2c.

SNMPv3 adopts user name and password authentication.

SNMPv1 and SNMPv2c adopt community name authentication. The SNMP packets containing invalid community names are discarded. SNMP community name is used to define the relationship between SNMP NMS and SNMP agent. Community name functions as password. It can limit accesses made by SNMP NMS to SNMP agent. You can perform the following community name-related configuration.

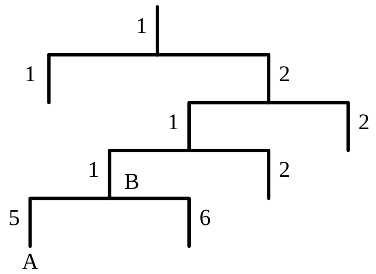
- Specifying MIB view that a community can access.

- Set the permission for a community to access an MIB object to be read-only or read-write. Communities with read-only permissions can only query the switch information, while those with read-write permission can configure the switch as well.
- Set the basic ACL specified by the community name.

Supported MIBs

An SNMP packet carries management variables with it. Management variable is used to describe the management objects of a switch. To uniquely identify the management objects of the switch, SNMP adopts a hierarchical naming scheme to organize the managed objects. It is like a tree, with each tree node representing a managed object, as shown in Figure 1-1. Each node in this tree can be uniquely identified by a path starting from the root.

Figure 1-1 Architecture of the MIB tree



MIB describes the hierarchical architecture of the tree and it is the set defined by the standard variables of the monitored network devices. In the above figure, the managed object B can be uniquely identified by a string of numbers {1.2.1.1}. The number string is the object identifier (OID) of the managed object.

Configuring Basic SNMP Functions

SNMPv3 configuration is quite different from that of SNMPv1 and SNMPv2c. Therefore, the configuration of basic SNMP functions is described by SNMP versions, as listed in the following two tables.

Follow these steps to configure basic SNMP functions (SNMPv1 and SNMPv2c):

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable SNMP agent	**snmp-agent**	Optional Disabled by default. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.
Set system information, and specify to enable SNMPv1 or SNMPv2c on the switch	**snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }	Required By default, the contact information for system maintenance is " 3Com Corporation.", the system location is " Marlborough, MA 01752 USA ", and the SNMP version is SNMPv3.

<table>
<tr><th colspan="3">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td rowspan="3">Set a community name and access permission</td><td>Direct configuration</td><td>Set a community name</td><td>snmp-agent community { read | write } community-name [acl acl-number | mib-view view-name]*</td><td rowspan="3">Required
• You can set an SNMPv1/SNMPv2c community name through direct configuration.
• Indirect configuration is compatible with SNMPv3. The added user is equal to the community name for SNMPv1 and SNMPv2c.
• You can choose either of them as needed.</td></tr>
<tr><td rowspan="2">Indirect configuration</td><td>Set an SNMP group</td><td>snmp-agent group { v1 | v2c } group-name [read-view read-view] [write-view write-view] [notify-view notify-view] [acl acl-number]</td></tr>
<tr><td>Add a user to an SNMP group</td><td>snmp-agent usm-user { v1 | v2c } user-name group-name [acl acl-number]</td></tr>
<tr><td colspan="3">Set the maximum size of an SNMP packet for SNMP agent to receive or send</td><td>snmp-agent packet max-size byte-count</td><td>Optional
1,500 bytes by default.</td></tr>
<tr><td colspan="3">Set the device engine ID</td><td>snmp-agent local-engineid engineid</td><td>Optional
By default, the device engine ID is “enterprise number + device information”.</td></tr>
<tr><td colspan="3">Create/Update the view information</td><td>snmp-agent mib-view { included | excluded } view-name oid-tree [mask mask-value]</td><td>Optional
By default, the view name is ViewDefault and OID is 1.</td></tr>
</table>

Follow these steps to configure basic SNMP functions (SNMPv3):

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable SNMP agent	**snmp-agent**	Optional Disabled by default. You can enable SNMP agent by executing this command or any of the commands used to configure SNMP agent.
Set system information and specify to enable SNMPv3 on the switch	**snmp-agent sys-info** { **contact** *sys-contact* | **location** sys-*location* | **version** { { **v1** | **v2c** | **v3** }* | **all** } }	Optional By default, the contact information for system maintenance is " 3Com Corporation.", the system location is " Marlborough, MA 01752 USA ", and the SNMP version is SNMPv3.
Set an SNMP group	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]	Required

To do…	Use the command…	Remarks
Encrypt a plain-text password to generate a cipher-text one	**snmp-agent calculate-password** *plain-password* **mode** { **md5** | **sha** } { **local-engineid | specified-engineid** *engineid* }	Optional This command is used if password in cipher-text is needed for adding a new user.
Add a user to an SNMP group	**snmp-agent usm-user v3** *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode des56** } *priv-password*]] [**acl** *acl-number*]	Required
Set the maximum size of an SNMP packet for SNMP agent to receive or send	**snmp-agent packet max-size** *byte-count*	Optional 1,500 bytes by default.
Set the device engine ID	**snmp-agent local-engineid** *engineid*	Optional By default, the device engine ID is "enterprise number + device information".
Create or update the view information	**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree* [**mask** *mask-value*]	Optional By default, the view name is ViewDefault and OID is 1.

Note

A Switch 4500 provides the following functions to prevent attacks through unused UDP ports.

- Executing the **snmp-agent** command or any of the commands used to configure SNMP agent enables the SNMP agent, and at the same opens UDP port 161 used by SNMP agents and the UDP port used by SNMP trap respectively.
- Executing the **undo snmp-agent** command disables the SNMP agent and closes UDP ports used by SNMP agent and SNMP trap as well.

Configuring Trap-Related Functions

Configuring Basic Trap Functions

traps refer to those sent by managed devices to the NMS without request. They are used to report some urgent and important events (for example, the rebooting of managed devices).

Note that basic SNMP configuration is performed before you configure basic trap function.

Follow these steps to configure basic trap function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Enable the switch to send traps to NMS</td><td>snmp-agent trap enable [configuration | flash | standard [authentication | coldstart | linkdown | linkup | warmstart]* | system]</td><td rowspan="4">Optional
By default, a port is enabled to send all types of traps.</td></tr>
<tr><td rowspan="3">Enable the port to send traps</td><td>Enter port view or interface view</td><td>interface interface-type interface-number</td></tr>
<tr><td>Enable the port or interface to send traps</td><td>enable snmp trap updown</td></tr>
<tr><td>Quit to system view</td><td>quit</td></tr>
<tr><td colspan="2">Set the destination for traps</td><td>snmp-agent target-host trap address udp-domain { ip-address } [udp-port port-number] params securityname security-string [v1 | v2c | v3 [authentication | privacy]]</td><td>Required</td></tr>
<tr><td colspan="2">Set the source address for traps</td><td>snmp-agent trap source interface-type interface-number</td><td>Optional</td></tr>
<tr><td colspan="2">Set the size of the queue used to hold the traps to be sent to the destination host</td><td>snmp-agent trap queue-size size</td><td>Optional
The default is 100.</td></tr>
<tr><td colspan="2">Set the aging time for traps</td><td>snmp-agent trap life seconds</td><td>Optional
120 seconds by default.</td></tr>
</table>

Configuring Extended Trap Function

The extended trap function refers to adding "interface description" and "interface type" into the linkUp/linkDown trap. When receiving this extended trap, NMS can immediately determine which interface on the device fails according to the interface description and type.

Follow these steps to configure extended trap function:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the extended trap function	**snmp-agent trap ifmib link extended**	Optional By default, the linkUp/linkDown trap adopts the standard format defined in IF-MIB. For details, refer to RFC 1213.

Enabling Logging for Network Management

Follow these steps to enable logging for network management:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Enable logging for network management	**snmp-agent log** { **set-operation** | **get-operation** | **all** }	Optional Disabled by default.

Note

- When SNMP logging is enabled on a device, SNMP logs are output to the information center of the device. With the output destinations of the information center set, the output destinations of SNMP logs will be decided.
- The severity level of SNMP logs is informational, that is, the logs are taken as general prompt information of the device. To view SNMP logs, you need to enable the information center to output system information with **informational** level.
- For detailed description on system information and information center, refer to the *Information Center Configuration* part in this manual.

Displaying SNMP

To do…	Use the command…	Remarks
Display the SNMP information about the current device	**display snmp-agent sys-info** [**contact** | **location** | **version**]*	Available in any view.
Display SNMP packet statistics	**display snmp-agent statistics**	
Display the engine ID of the current device	**display snmp-agent** { **local-engineid** | **remote-engineid** }	
Display group information about the device	**display snmp-agent group** [*group-name*]	
Display SNMP user information	**display snmp-agent usm-user** [**engineid** *engineid* | **username** *user-name* | **group** *group-name*]*	
Display trap list information	**display snmp-agent trap-list**	
Display the currently configured community name	**display snmp-agent community** [**read** | **write**]	
Display the currently configured MIB view	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]	

SNMP Configuration Example

SNMP Configuration Example

Network requirements

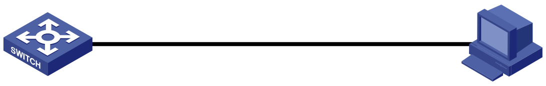
- An NMS and Switch A (SNMP agent) are connected through the Ethernet. The IP address of the NMS is 10.10.10.1 and that of the VLAN interface on Switch A is 10.10.10.2.

- Perform the following configuration on Switch A: setting the community name and access permission, administrator ID, contact and switch location, and enabling the switch to sent traps.

Thus, the NMS is able to access Switch A and receive the traps sent by Switch A.

Network diagram

Figure 1-2 Network diagram for SNMP configuration



Network procedure

Enable SNMP agent, and set the SNMPv1 and SNMPv2c community names.

```
<Sysname> system-view
[Sysname] snmp-agent
[Sysname] snmp-agent sys-info version all
[Sysname] snmp-agent community read public
[Sysname] snmp-agent community write private
```

Set the access right of the NMS to the MIB of the SNMP agent.

```
[Sysname] snmp-agent mib-view include internet 1.3.6.1
```

For SNMPv3, set:

- SNMPv3 group and user
- security to the level of needing authentication and encryption
- authentication protocol to **HMAC-MD5**
- authentication password to **passmd5**
- encryption protocol to **DES**
- encryption password to **cfb128cfb128**

```
[Sysname] snmp-agent group v3 managev3group privacy write-view internet
[Sysname] snmp-agent usm-user v3 managev3user managev3group authentication-mode md5 passmd5
privacy-mode des56 cfb128cfb128
```

Set the VLAN-interface 2 as the interface used by NMS. Add port Ethernet 1/0/2, which is to be used for network management, to VLAN 2. Set the IP address of VLAN-interface 2 as 10.10.10.2.

```
[Sysname] vlan 2
[Sysname-vlan2] port Ethernet 1/0/2
[Sysname-vlan2] quit
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] ip address 10.10.10.2 255.255.255.0
[Sysname-Vlan-interface2] quit
```

Enable the SNMP agent to send traps to the NMS whose IP address is 10.10.10.1. The SNMP community name to be used is **public**.

```
[Sysname] snmp-agent trap enable standard authentication
[Sysname] snmp-agent trap enable standard coldstart
[Sysname] snmp-agent trap enable standard linkup
```

```
[Sysname] snmp-agent trap enable standard linkdown
[Sysname] snmp-agent target-host trap address udp-domain 10.10.10.1 udp-port 5000 params
securityname public
```

Configuring the NMS

Authentication-related configuration on an NMS must be consistent with that of the devices for the NMS to manage the devices successfully. For more information, refer to the corresponding manuals of 3Com's NMS products.

You can query and configure an Ethernet switch through the NMS.

2 RMON Configuration

When configuring RMON, go to these sections for information you are interested in:

Introduction to RMON

Remote Monitoring (RMON) is a kind of MIB defined by Internet Engineering Task Force (IETF). It is an important enhancement made to MIB II standards. RMON is mainly used to monitor the data traffic across a network segment or even the entire network, and is currently a commonly used network management standard.

An RMON system comprises of two parts: the network management station (NMS) and the agents running on network devices. RMON agents operate on network monitors or network probes to collect and keep track of the statistics of the traffic across the network segments to which their ports connect, such as the total number of the packets on a network segment in a specific period of time and the total number of packets successfully sent to a specific host.

- RMON is fully based on SNMP architecture. It is compatible with the current SNMP implementations.
- RMON enables SNMP to monitor remote network devices more effectively and actively, thus providing a satisfactory means of monitoring remote subnets.
- With RMON implemented, the communication traffic between NMS and SNMP agents can be reduced, thus facilitating the management of large-scale internetworks.

Working Mechanism of RMON

RMON allows multiple monitors. It can collect data in the following two ways:

- Using the dedicated RMON probes. When an RMON system operates in this way, the NMS directly obtains management information from the RMON probes and controls the network resources. In this case, all information in the RMON MIB can be obtained.
- Embedding RMON agents into network devices (such as routers, switches and hubs) directly to make the latter capable of RMON probe functions. When an RMON system operates in this way, the NMS collects network management information by exchanging information with the SNMP agents using the basic SNMP commands. However, this way depends on device resources heavily and an NMS operating in this way can only obtain the information about these four groups (instead of all the information in the RMON MIB): alarm group, event group, history group, and statistics group.

A Switch 4500 implements RMON in the second way. With an RMON agent embedded in, A Switch 4500 can serve as a network device with the RMON probe function. Through the RMON-capable SNMP agents running on the Ethernet switch, an NMS can obtain the information about the total traffic, error

statistics and performance statistics of the network segments to which the ports of the managed network devices are connected. Thus, the NMS can further manage the networks.

Commonly Used RMON Groups

Event group

Event group is used to define the indexes of events and the processing methods of the events. The events defined in an event group are mainly used by entries in the alarm group and extended alarm group to trigger alarms.

You can specify a network device to act in one of the following ways in response to an event:

- Logging the event
- Sending traps to the NMS
- Logging the event and sending traps to the NMS
- No processing

Alarm group

RMON alarm management enables monitoring on specific alarm variables (such as the statistics of a port). When the value of a monitored variable exceeds the threshold, an alarm event is generated, which then triggers the network device to act in the way defined in the events. Events are defined in event groups.

With an alarm entry defined in an alarm group, a network device performs the following operations accordingly:

- Sampling the defined alarm variables periodically
- Comparing the samples with the threshold and triggering the corresponding events if the former exceed the latter

Extended alarm group

With extended alarm entry, you can perform operations on the samples of alarm variables and then compare the operation results with the thresholds, thus implement more flexible alarm functions.

With an extended alarm entry defined in an extended alarm group, the network devices perform the following operations accordingly:

- Sampling the alarm variables referenced in the defined extended alarm expressions periodically
- Performing operations on the samples according to the defined expressions
- Comparing the operation results with the thresholds and triggering corresponding events if the operation result exceeds the thresholds.

History group

After a history group is configured, the Ethernet switch collects network statistics information periodically and stores the statistics information temporarily for later use. A history group can provide the history data of the statistics on network segment traffic, error packets, broadcast packets, and bandwidth utilization.

With the history data management function, you can configure network devices to collect history data, sample and store data of a specific port periodically.

Statistics group

Statistics group contains the statistics of each monitored port on a switch. An entry in a statistics group is an accumulated value counting from the time when the statistics group is created.

The statistics include the number of the following items: collisions, packets with Cyclic Redundancy Check (CRC) errors, undersize (or oversize) packets, broadcast packets, multicast packets, and received bytes and packets.

With the RMON statistics management function, you can monitor the use of a port and make statistics on the errors occurred when the ports are being used.

RMON Configuration

Before performing RMON configuration, make sure the SNMP agents are correctly configured. For the information about SNMP agent configuration, refer to section Configuring Basic SNMP Functions.

Follow these steps to configure RMON:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Add an event entry	**rmon event** *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]	Optional
Add an alarm entry	**rmon alarm** *entry-number alarm-variable sampling-time* { **delta** | **absolute** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* [**owner** *text*]	Optional Before adding an alarm entry, you need to use the **rmon event** command to define the event to be referenced by the alarm entry.
Add an extended alarm entry	**rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-timer* { **delta** | **absolute** | **changeratio** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]	Optional Before adding an extended alarm entry, you need to use the **rmon event** command to define the event to be referenced by the extended alarm entry.
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Add a history entry	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]	Optional
Add a statistics entry	**rmon statistics** *entry-number* [**owner** *text*]	Optional

Note

- The **rmon alarm** and **rmon prialarm** commands take effect on existing nodes only.
- For each port, only one RMON statistics entry can be created. That is, if an RMON statistics entry is already created for a given port, you will fail to create another statistics entry with a different index for the same port.

Displaying RMON

To do…	Use the command…	Remarks
Display RMON statistics	**display rmon statistics** [*interface-type interface-number* | **unit** *unit-number*]	Available in any view.
Display RMON history information	**display rmon history** [*interface-type interface-number* | **unit** *unit-number*]	
Display RMON alarm information	**display rmon alarm** [*entry-number*]	
Display extended RMON alarm information	**display rmon prialarm** [*prialarm-entry-number*]	
Display RMON events	**display rmon event** [*event-entry*]	
Display RMON event logs	**display rmon eventlog** [*event-entry*]	

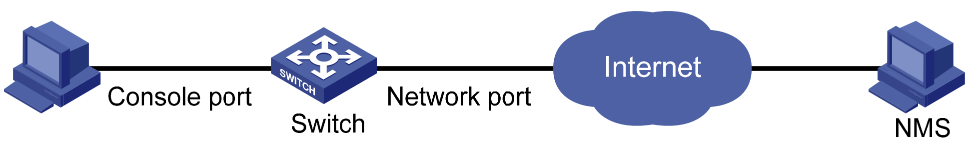
RMON Configuration Example

Network requirements

- The switch to be tested is connected to a remote NMS through the Internet. Ensure that the SNMP agents are correctly configured before performing RMON configuration.
- Create an entry in the extended alarm table to monitor the information of statistics on the Ethernet port, if the change rate of which exceeds the set threshold, the alarm events will be triggered.

Network diagram

Figure 2-1 Network diagram for RMON configuration



Configuration procedures

Add the statistics entry numbered 1 to take statistics on Ethernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] rmon statistics 1
```

```
[Sysname-Ethernet1/0/1] quit
```

Add the event entries numbered 1 and 2 to the event table, which will be triggered by the following extended alarm.

```
[Sysname] rmon event 1 log
[Sysname] rmon event 2 trap 10.21.30.55
```

Add an entry numbered 2 to the extended alarm table to allow the system to calculate the alarm variables with the (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1) formula to get the numbers of all the oversize and undersize packets received by Ethernet 1/0/1 that are in correct data format and sample it in every 10 seconds. When the change ratio between samples reaches the rising threshold of 50, event 1 is triggered; when the change ratio drops under the falling threshold, event 2 is triggered.

```
[Sysname] rmon prialarm 2 (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1) test 10
changeratio rising_threshold 50 1 falling_threshold 5 2 entrytype forever owner user1
```

Display the RMON extended alarm entry numbered 2.

```
[Sysname] display rmon prialarm 2
Prialarm table 2 owned by user1 is VALID.
  Samples type            : changeratio
  Variable formula : (.1.3.6.1.2.1.16.1.1.1.9.1+.1.3.6.1.2.1.16.1.1.1.10.1)
  Description             : test
  Sampling interval      : 10(sec)
  Rising threshold       : 100(linked with event 1)
  Falling threshold      : 10(linked with event 2)
  When startup enables  : risingOrFallingAlarm
  This entry will exist : forever.
  Latest value            : 0
```

Table of Contents

1 NTP Configuration

When configuring NTP, go to these sections for information you are interested in:

Introduction to NTP

Network Time Protocol (NTP) is a time synchronization protocol defined in RFC 1305. It is used for time synchronization between a set of distributed time servers and clients. Carried over UDP, NTP transmits packets through UDP port 123.

NTP is intended for time synchronization between all devices that have clocks in a network so that the clocks of all devices can keep consistent. Thus, the devices can provide multiple unified-time-based applications (see section Applications of NTP).

A local system running NTP can not only be synchronized by other clock sources, but also serve as a clock source to synchronize other clocks. Besides, it can synchronize, or be synchronized by other systems by exchanging NTP messages.

Applications of NTP

As setting the system time manually in a network with many devices leads to a lot of workload and cannot ensure accuracy, it is unfeasible for an administrator to perform the operation. However, an administrator can synchronize the clocks of devices in a network with required accuracy by performing NTP configuration.

NTP is mainly applied to synchronizing the clocks of all devices in a network. For example:

- In network management, the analysis of the log information and debugging information collected from different devices is meaningful and valid only when network devices that generate the information adopts the same time.
- The billing system requires that the clocks of all network devices be consistent.
- Some functions, such as restarting all network devices in a network simultaneously require that they adopt the same time.
- When multiple systems cooperate to handle a rather complex transaction, they must adopt the same time to ensure a correct execution order.
- To perform incremental backup operations between a backup server and a host, you must make sure they adopt the same time.

NTP has the following advantages:

- Defining the accuracy of clocks by stratum to synchronize the clocks of all devices in a network quickly
- Supporting access control (see section Configuring Access Control Right) and MD5 encrypted authentication (see section Configuring NTP Authentication)
- Sending protocol packets in unicast, multicast, or broadcast mode

---

Note

- The clock stratum determines the accuracy, which ranges from 1 to 16. The stratum of a reference clock ranges from 1 to 15. The clock accuracy decreases as the stratum number increases. A stratum 16 clock is in the unsynchronized state and cannot serve as a reference clock.
- The local clock of an S4500 Ethernet switch cannot be set as a reference clock. It can serve as a reference clock source to synchronize the clock of other devices only after it is synchronized.

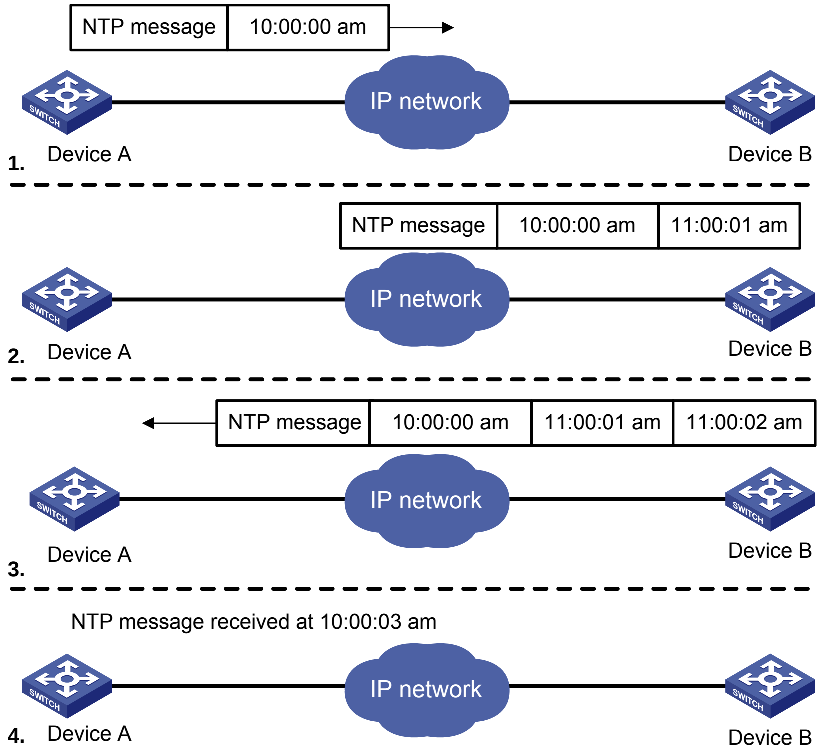
Implementation Principle of NTP

Figure 1-1 shows the implementation principle of NTP.

Ethernet switch A (Device A) is connected to Ethernet switch B (Device B) through Ethernet ports. Both having their own system clocks, they need to synchronize the clocks of each other through NTP. To help you to understand the implementation principle, we suppose that:

- Before the system clocks of Device A and Device B are synchronized, the clock of Device A is set to 10:00:00 am, and the clock of Device B is set to 11:00:00 am.
- Device B serves as the NTP server, that is, the clock of Device A will be synchronized to that of Device B.
- It takes one second to transfer an NTP message from Device A to Device B or from Device B to Device A.

Figure 1-1 Implementation principle of NTP



The procedure of synchronizing the system clock is as follows:

- Device A sends an NTP message to Device B, with a timestamp 10:00:00 am (T_1) identifying when it is sent.
- When the message arrives at Device B, Device B inserts its own timestamp 11:00:01 am (T_2) into the packet.
- When the NTP message leaves Device B, Device B inserts its own timestamp 11:00:02 am (T_3) into the packet.
- When Device A receives the NTP message, the local time of Device A is 10:00:03am (T4).

At this time, Device A has enough information to calculate the following two parameters:

- Delay for an NTP message to make a round trip between Device A and Device B:

$$\text{Delay} = (T_4 - T_1) - (T_3 - T_2).$$

- Time offset of Device A relative to Device B:

$$\text{Offset} = ((T_2 - T_1) + (T_3 - T_4))/2.$$

Device A can then set its own clock according to the above information to synchronize its clock to that of Device B.

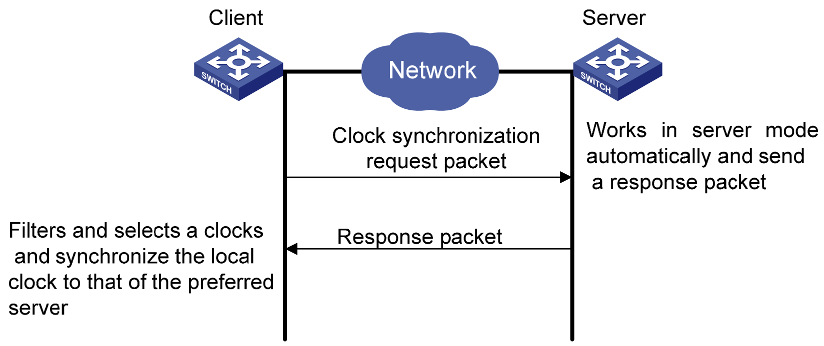
For detailed information, refer to RFC 1305.

NTP Implementation Modes

According to the network structure and the position of the local Ethernet switch in the network, the local Ethernet switch can work in multiple NTP modes to synchronize the clock.

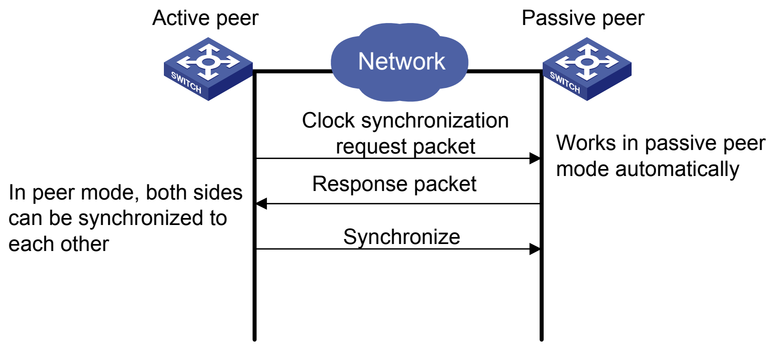
Server/client mode

Figure 1-2 Server/client mode



Symmetric peer mode

Figure 1-3 Symmetric peer mode

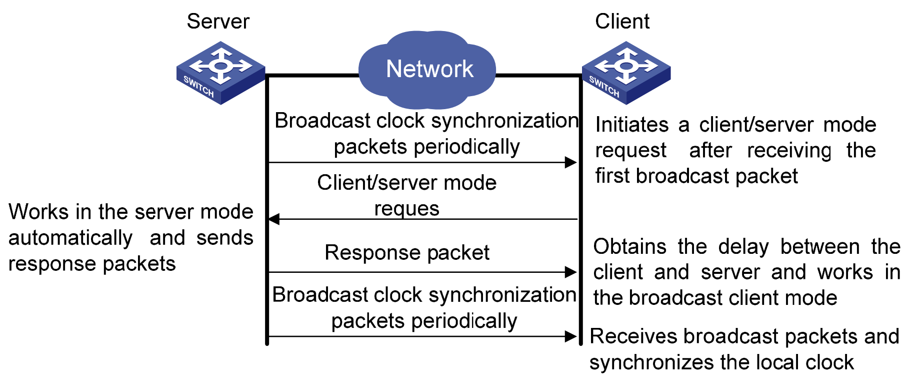


In the symmetric peer mode, the local S4500 Ethernet switch serves as the symmetric-active peer and sends clock synchronization request first, while the remote server serves as the symmetric-passive peer automatically.

If both of the peers have reference clocks, the one with a smaller stratum number is adopted.

Broadcast mode

Figure 1-4 Broadcast mode



Multicast mode

Figure 1-5 Multicast mode

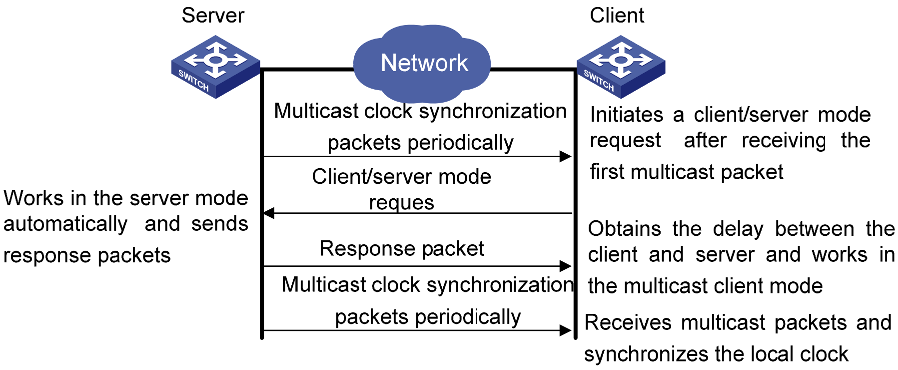


Table 1-1 describes how the above mentioned NTP modes are implemented on 3Com S4500 series Ethernet switches.

Table 1-1 NTP implementation modes on 3Com S4500 series Ethernet switches

NTP implementation mode	Configuration on S4500 series switches
Server/client mode	Configure the local S4500 Ethernet switch to work in the NTP client mode. In this mode, the remote server serves as the local time server, while the local switch serves as the client.
Symmetric peer mode	Configure the local S4500 switch to work in NTP symmetric peer mode. In this mode, the remote server serves as the symmetric-passive peer of the S4500 switch, and the local switch serves as the symmetric-active peer.
Broadcast mode	• Configure the local S4500 Ethernet switch to work in NTP broadcast server mode. In this mode, the local switch broadcasts NTP messages through the VLAN interface configured on the switch. • Configure the S4500 switch to work in NTP broadcast client mode. In this mode, the local S4500 switch receives broadcast NTP messages through the VLAN interface configured on the switch.
Multicast mode	• Configure the local S4500 Ethernet switch to work in NTP multicast server mode. In this mode, the local switch sends multicast NTP messages through the VLAN interface configured on the switch. • Configure the local S4500 Ethernet switch to work in NTP multicast client mode. In this mode, the local switch receives multicast NTP messages through the VLAN interface configured on the switch.

Caution

- When a 3Com S4500 Ethernet switch works in server mode or symmetric passive mode, you need not to perform related configurations on this switch but do that on the client or the symmetric-active peer.
- The NTP server mode, NTP broadcast mode, or NTP multicast mode takes effect only after the local clock of the 3Com S4500 Ethernet switch has been synchronized.
- When symmetric peer mode is configured on two Ethernet switches, to synchronize the clock of the two switches, make sure at least one switch's clock has been synchronized.

NTP Configuration Task List

Complete the following tasks to configure NTP:

Task	Remarks
Configuring NTP Implementation Modes	Required
Configuring Access Control Right	Optional
Configuring NTP Authentication	Optional
Configuring Optional NTP Parameters	Optional
Displaying NTP Configuration	Optional

Configuring NTP Implementation Modes

An S4500 Ethernet switch can work in one of the following NTP modes:

- Configuring NTP Server/Client Mode
- Configuring the NTP Symmetric Peer Mode
- Configuring NTP Broadcast Mode
- Configuring NTP Multicast Mode

Note

To protect unused sockets against attacks by malicious users and improve security, 3Com S4500 series Ethernet switches provide the following functions:

- UDP port 123 is opened only when the NTP feature is enabled.
- UDP port 123 is closed as the NTP feature is disabled.

These functions are implemented as follows:

- Execution of one of the **ntp-service unicast-server**, **ntp-service unicast-peer**, **ntp-service broadcast-client**, **ntp-service broadcast-server**, **ntp-service multicast-client**, and **ntp-service multicast-server** commands enables the NTP feature and opens UDP port 123 at the same time.
- Execution of the **undo** form of one of the above six commands disables all implementation modes of the NTP feature and closes UDP port 123 at the same time.

Configuring NTP Server/Client Mode

For switches working in the server/client mode, you only need to perform configurations on the clients, and not on the servers.

Follow these steps to configure an NTP client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure an NTP client	**ntp-service unicast-server** { *remote-ip* | *server-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface Vlan-interface** *vlan-id* | **version** *number*]*	Required By default, the switch is not configured to work in the NTP client mode.

Note

- The remote server specified by *remote-ip* or *server-name* serves as the NTP server, and the local switch serves as the NTP client. The clock of the NTP client will be synchronized by but will not synchronize that of the NTP server.
- *remote-ip* cannot be a broadcast address, a multicast address or the IP address of the local clock.
- After you specify an interface for sending NTP messages through the **source-interface** keyword, the source IP address of the NTP message will be configured as the primary IP address of the specified interface.
- A switch can act as a server to synchronize the clock of other switches only after its clock has been synchronized. If the clock of a server has a stratum level lower than or equal to that of a client's clock, the client will not synchronize its clock to the server's.
- You can configure multiple servers by repeating the **ntp-service unicast-server** command. The client will choose the optimal reference source.

Configuring the NTP Symmetric Peer Mode

For switches working in the symmetric peer mode, you need to specify a symmetric-passive peer on the symmetric-active peer.

Follow these steps to configure a symmetric-active switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Specify a symmetric-passive peer for the switch	**ntp-service unicast-peer** { *remote-ip* | *peer-name* } [**authentication-keyid** *key-id* | **priority** | **source-interface Vlan-interface** *vlan-id* | **version** *number*]*	Required By default, a switch is not configured to work in the symmetric mode.

Note

- In the symmetric peer mode, you need to execute the related NTP configuration commands (refer to section Configuring NTP Implementation Modes for details) to enable NTP on a symmetric-passive peer; otherwise, the symmetric-passive peer will not process NTP messages from the symmetric-active peer.
- The remote device specified by *remote-ip* or *peer-name* serves as the peer of the local Ethernet switch, and the local switch works in the symmetric-active mode. In this case, the clock of the local switch and that of the remote device can be synchronized to each other.
- *remote-ip* must not be a broadcast address, a multicast address or the IP address of the local clock.
- After you specify an interface for sending NTP messages through the **source-interface** keyword, the source IP address of the NTP message will be configured as the IP address of the specified interface.
- Typically, the clock of at least one of the symmetric-active and symmetric-passive peers should be synchronized first; otherwise the clock synchronization will not proceed.
- You can configure multiple symmetric-passive peers for the local switch by repeating the **ntp-service unicast-peer** command. The clock of the peer with the smallest stratum will be chosen to synchronize with the local clock of the switch.

Configuring NTP Broadcast Mode

For switches working in the broadcast mode, you need to configure both the server and clients. The broadcast server periodically sends NTP broadcast messages to the broadcast address 255.255.255.255. The switches working in the NTP broadcast client mode will respond to the NTP messages, so as to start the clock synchronization.

Note

A broadcast server can synchronize broadcast clients only after its clock has been synchronized.

Configuring a switch to work in the NTP broadcast server mode

Follow these steps to configure a switch to work in the NTP broadcast server mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the switch to work in the NTP broadcast server mode	**ntp-service broadcast-server** [**authentication-keyid** *key-id* | **version** *number*]*	Required Not configured by default.

Configuring a switch to work in the NTP broadcast client mode

Follow these steps to configure a switch to work in the NTP broadcast client mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the switch to work in the NTP broadcast client mode	**ntp-service broadcast-client**	Required Not configured by default.

Configuring NTP Multicast Mode

For switches working in the multicast mode, you need to configure both the server and clients. The multicast server periodically sends NTP multicast messages to multicast clients. The switches working in the NTP multicast client mode will respond to the NTP messages, so as to start the clock synchronization.

Note

- A multicast server can synchronize multicast clients only after its clock has been synchronized.
- An S4500 series switch working in the multicast server mode supports up to 1,024 multicast clients.

Configuring a switch to work in the multicast server mode

Follow these steps to configure a switch to work in the NTP multicast server mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the switch to work in the NTP multicast server mode	**ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*]*	Required Not configured by default.

Configuring a switch to work in the multicast client mode

Follow these steps to configure a switch to work in the NTP multicast client mode:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Configure the switch to work in the NTP multicast client mode	**ntp-service multicast-client** [*ip-address*]	Required Not configured by default.

Configuring Access Control Right

With the following command, you can configure the NTP service access-control right to the local switch for a peer device. There are four access-control rights, as follows:

- **query**: Control query right. This level of right permits the peer device to perform control query to the NTP service on the local device but does not permit the peer device to synchronize its clock to the local device. The so-called "control query" refers to query of state of the NTP service, including alarm information, authentication status, clock source information, and so on.
- **synchronization**: Synchronization right. This level of right permits the peer device to synchronize its clock to the local switch but does not permit the peer device to perform control query.
- **server**: Server right. This level of right permits the peer device to perform synchronization and control query to the local switch but does not permit the local switch to synchronize its clock to the peer device.
- **peer**: Peer access. This level of right permits the peer device to perform synchronization and control query to the local switch and also permits the local switch to synchronize its clock to the peer device.

NTP service access-control rights from the highest to the lowest are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will perform an access-control right match in this order and use the first matched right.

Configuration Prerequisites

Prior to configuring the NTP service access-control right to the local switch for peer devices, you need to create and configure an ACL associated with the access-control right. For the configuration of ACL, refer to *ACL Configuration* in *Security Volume*.

Configuration Procedure

Follow these steps to configure the NTP service access-control right to the local device for peer devices:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the NTP service access-control right to the local switch for peer devices	**ntp-service access** { **peer** | **server** | **synchronization** | **query** } *acl-number*	Optional **peer** by default

Note

The access-control right mechanism provides only a minimum degree of security protection for the local switch. A more secure method is identity authentication.

Configuring NTP Authentication

In networks with higher security requirements, the NTP authentication function must be enabled to run NTP. Through password authentication on the client and the server, the clock of the client is synchronized only to that of the server that passes the authentication. This improves network security. Table 1-2 shows the roles of devices in the NTP authentication function.

Table 1-2 Description on the roles of devices in NTP authentication function

Role of device	Working mode
Client	Client in the server/client mode
	Client in the broadcast mode
	Client in the multicast mode
	Symmetric-active peer in the symmetric peer mode
Server	Server in the server/client mode
	Server in the broadcast mode
	Server in the multicast mode
	Symmetric-passive peer in the symmetric peer mode

Configuration Prerequisites

NTP authentication configuration involves:

- Configuring NTP authentication on the client
- Configuring NTP authentication on the server

Observe the following principles when configuring NTP authentication:

- If the NTP authentication function is not enabled on the client, the clock of the client can be synchronized to a server no matter whether the NTP authentication function is enabled on the server (assuming that other related configurations are properly performed).
- For the NTP authentication function to take effect, a trusted key needs to be configured on both the client and server after the NTP authentication is enabled on them.
- The local clock of the client is only synchronized to the server that provides a trusted key.
- In addition, for the server/client mode and the symmetric peer mode, you need to associate a specific key on the client (the symmetric-active peer in the symmetric peer mode) with the corresponding NTP server (the symmetric-passive peer in the symmetric peer mode); for the NTP broadcast/multicast mode, you need to associate a specific key on the broadcast/multicast server with the corresponding NTP broadcast/multicast client. Otherwise, NTP authentication cannot be enabled normally.
- Configurations on the server and the client must be consistent.

Configuration Procedure

Configuring NTP authentication on the client

Follow these steps to configure NTP authentication on the client:

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="2">Enable the NTP authentication function</td><td>ntp-service authentication enable</td><td>Required
Disabled by default.</td></tr>
<tr><td colspan="2">Configure the NTP authentication key</td><td>ntp-service authentication-keyid key-id authentication-model md5 value</td><td>Required
By default, no NTP authentication key is configured.</td></tr>
<tr><td colspan="2">Configure the specified key as a trusted key</td><td>ntp-service reliable authentication-keyid key-id</td><td>Required
By default, no trusted key is configured.</td></tr>
<tr><td rowspan="2">Associate the specified key with the corresponding NTP server</td><td>Configure on the client in the server/client mode</td><td>ntp-service unicast-server { remote-ip | server-name } authentication-keyid key-id</td><td rowspan="2">Required
For the client in the NTP broadcast/multicast mode, you just need to associate the specified key with the client on the corresponding server.</td></tr>
<tr><td>Configure on the symmetric-active peer in the symmetric peer mode</td><td>ntp-service unicast-peer { remote-ip | peer-name } authentication-keyid key-id</td></tr>
</table>

Note

NTP authentication requires that the authentication keys configured for the server and the client be the same. Besides, the authentication keys must be trusted keys. Otherwise, the clock of the client cannot be synchronized with that of the server.

Configuring NTP authentication on the server

Follow these steps to configure NTP authentication on the server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable NTP authentication	**ntp-service authentication enable**	Required Disabled by default.
Configure an NTP authentication key	**ntp-service authentication-keyid** *key-id* **authentication-mode md5** *value*	Required By default, no NTP authentication key is configured.

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Configure the specified key as a trusted key</td><td>ntp-service reliable authentication-keyid key-id</td><td>Required
By default, no trusted authentication key is configured.</td></tr>
<tr><td colspan="2">Enter VLAN interface view</td><td>interface Vlan-interface vlan-id</td><td>—</td></tr>
<tr><td rowspan="2">Associate the specified key with the corresponding broadcast/multicast client</td><td>Configure on the NTP broadcast server</td><td>ntp-service broadcast-server authentication-keyid key-id</td><td rowspan="2">• In NTP broadcast server mode and NTP multicast server mode, you need to associate the specified key with the corresponding broadcast/multicast client
• You can associate an NTP broadcast/multicast client with an authentication key while configuring NTP mode. You can also use this command to associate them after configuring the NTP mode.</td></tr>
<tr><td>Configure on the NTP multicast server</td><td>ntp-service multicast-server authentication-keyid key-id</td></tr>
</table>

Note

The procedure for configuring NTP authentication on the server is the same as that on the client. Besides, the client and the server must be configured with the same authentication key.

Configuring Optional NTP Parameters

Complete the following tasks to configure optional NTP parameters:

Task	Remarks
Configuring an Interface on the Local Switch to Send NTP messages	Optional
Configuring the Number of Dynamic Sessions Allowed on the Local Switch	Optional
Disabling an Interface from Receiving NTP messages	Optional

Configuring an Interface on the Local Switch to Send NTP messages

Follow these steps to configure an interface on the local switch to send NTP messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure an interface on the local switch to send NTP messages	**ntp-service source-interface Vlan-interface** *vlan-id*	Required

Caution

If you have specified an interface in the **ntp-service unicast-server** or **ntp-service unicast-peer** command, this interface will be used for sending NTP messages.

Configuring the Number of Dynamic Sessions Allowed on the Local Switch

A single device can have a maximum of 128 associations at the same time, including static associations and dynamic associations. A static association refers to an association that a user has manually created by using an NTP command, while a dynamic association is a temporary association created by the system during operation. A dynamic association will be removed if the system fails to receive messages from it over a specific long time.

In the server/client mode, for example, when you carry out a command to synchronize the time to a server, the system will create a static association, and the server will just respond passively upon the receipt of a message, rather than creating an association (static or dynamic). In the symmetric mode, static associations will be created at the symmetric-active peer side, and dynamic associations will be created at the symmetric-passive peer side; In the broadcast or multicast mode, static associations will be created at the server side, and dynamic associations will be created at the client side.

Follow these steps to configure the number of dynamic sessions allowed on the local switch:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the maximum number of dynamic sessions that can be established on the local switch	**ntp-service max-dynamic-sessions** *number*	Required By default, up to 100 dynamic sessions can be established locally.

Disabling an Interface from Receiving NTP messages

Follow these steps to disable an interface from receiving NTP messages:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface Vlan-interface** *vlan-id*	—
Disable an interface from receiving NTP messages	**ntp-service in-interface disable**	Required By default, a VLAN interface receives NTP messages.

Displaying NTP Configuration

To do…	Use the command…	Remarks
Display the status of NTP services	**display ntp-service status**	Available in any view

To do…	Use the command…	Remarks
Display the information about the sessions maintained by NTP	**display ntp-service sessions** [**verbose**]	
Display the brief information about NTP servers along the path from the local device to the reference clock source	**display ntp-service trace**	

Configuration Examples

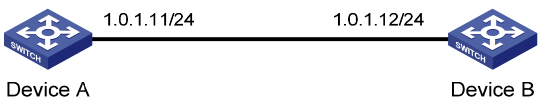
Configuring NTP Server/Client Mode

Network requirements

- The local clock of Device A (a switch) is to be used as a master clock, with the stratum level of 2.
- Device A is used as the NTP server of Device B (an S4500 Ethernet switch)
- Configure Device B to work in the client mode, and then Device A will automatically work in the server mode.

Network diagram

Figure 1-6 Network diagram for the NTP server/client mode configuration



Configuration procedure

Perform the following configurations on Device B.

View the NTP status of Device B before synchronization.

```
<DeviceB> display ntp-service status
 Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900 (00000000.00000000)
```

Set Device A as the NTP server of Device B.

```
<DeviceB> system-view
[DeviceB] ntp-service unicast-server 1.0.1.11
```

(After the above configurations, Device B is synchronized to Device A.) View the NTP status of Device B.

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 0.66 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)
```

The above output information indicates that Device B is synchronized to Device A, and the stratum level of its clock is 3, one level lower than that of Device A.

View the information about NTP sessions of Device B. (You can see that Device B establishes a connection with Device A.)

```
[DeviceB] display ntp-service sessions
     source         reference       stra reach poll  now offset  delay disper
**************************************************************************
[12345]1.0.1.11    127.127.1.0     2    1   64    1   350.1   15.1    0.0
note:  1  source(master),2  source(peer),3  selected,4  candidate,5  configured  Total
associations :  1
```

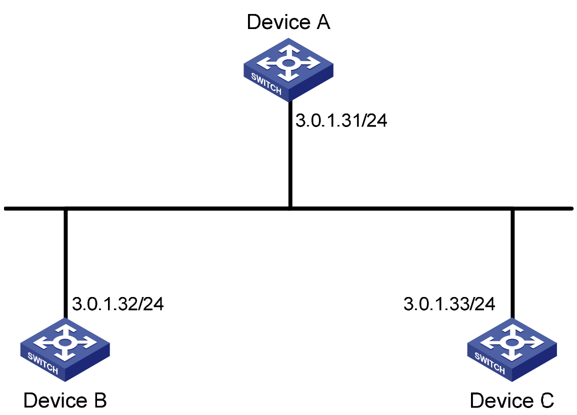
Configuring NTP Symmetric Peer Mode

Network requirements

- The local clock of Device A is set as the NTP master clock, with the clock stratum level of 2.
- Device C (an S4500 Ethernet switch) uses Device A as the NTP server, and Device A works in server mode automatically.
- The local clock of Device B is set as the NTP master clock, with the clock stratum level of 1. Set Device C as the peer of Device B.

Network diagram

Figure 1-7 Network diagram for NTP peer mode configuration



Configuration procedure

- Configure Device C.

Set Device A as the NTP server.

```
<DeviceC> system-view
[DeviceC] ntp-service unicast-server 3.0.1.31
```

- Configure Device B (after the Device C is synchronized to Device A).

Enter system view.

```
<DeviceB> system-view
```

Set Device C as the peer of Device B.

```
[DeviceB] ntp-service unicast-peer 3.0.1.33
```

Device C and Device B are symmetric peers after the above configuration. Device B works in symmetric active mode, while Device C works in symmetric passive mode. Because the stratum level of the local clock of Device B is 1, and that of Device C is 3, the clock of Device C is synchronized to that of Device B.

View the status of Device C after the clock synchronization.

```
[DeviceC] display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
 Reference clock ID: 3.0.1.32
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 0.66 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)
```

The output information indicates that the clock of Device C is synchronized to that of Device B and the stratum level of its local clock is 2, one level lower than Device B.

View the information about the NTP sessions of Device C (you can see that a connection is established between Device C and Device B).

```
[DeviceC] display ntp-service sessions
     source          reference        stra reach poll  now offset  delay disper
*************************************************************************
[1234]3.0.1.32    LOCL               1    95   64   42  -14.3   12.9    2.7
[25]3.0.1.31    127.127.1.0          2     1   64    1 4408.6   38.7    0.0
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  2
```

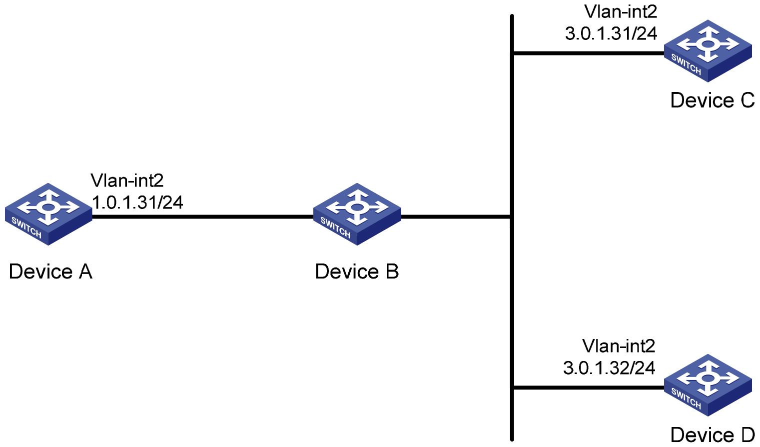
Configuring NTP Broadcast Mode

Network requirements

- The local clock of Device C is set as the NTP master clock, with a stratum level of 2. Configure Device C to work in the NTP broadcast server mode and send NTP broadcast messages through VLAN-interface 2.
- Device A and Device D are two S4500 Ethernet switches. Configure Device A and Device D to work in the NTP broadcast client mode and listen to broadcast messages through their own VLAN-interface 2.

Network diagram

Figure 1-8 Network diagram for the NTP broadcast mode configuration



Configuration procedure

- Configure Device C.

Enter system view.

```
<DeviceC> system-view
```

Set Device C as the broadcast server, which sends broadcast messages through VLAN-interface 2.

```
[DeviceC] interface Vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service broadcast-server
```

- Configure Device A. (Perform the same configuration on Device D.)

Enter system view.

```
<DeviceA> system-view
```

Set Device A as a broadcast client.

```
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service broadcast-client
```

After the above configurations, Device A and Device D will listen to broadcast messages through their own VLAN-interface 2, and Device C will send broadcast messages through VLAN-interface 2. Because Device A and Device C do not share the same network segment, Device A cannot receive broadcast messages from Device C, while Device D is synchronized to Device C after receiving broadcast messages from Device C.

View the NTP status of Device D after the clock synchronization.

```
[DeviceD] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)
```

The output information indicates that Device D is synchronized to Device C, with the clock stratum level of 3, one level lower than that of Device C.

View the information about the NTP sessions of Device D and you can see that a connection is established between Device D and Device C.

```
[DeviceD] display ntp-service sessions
    source          reference       stra reach poll  now offset   delay disper
**************************************************************************
[1234]3.0.1.31     127.127.1.0      2    1    64   377    26.1   199.53   9.7
note:  1  source(master),2  source(peer),3  selected,4  candidate,5  configured  Total
associations :  1
```

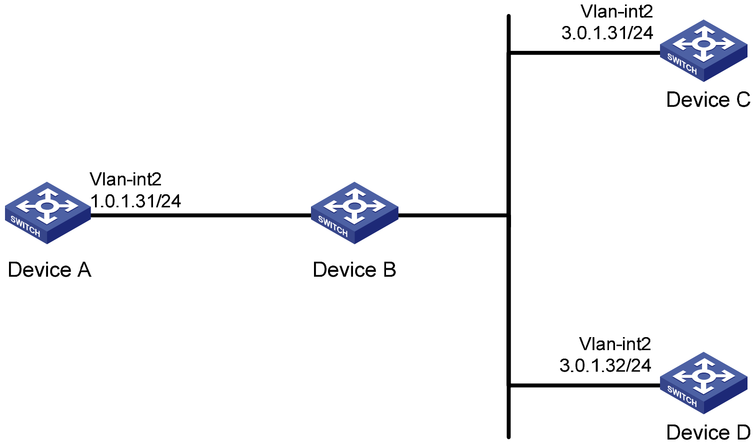
Configuring NTP Multicast Mode

Network requirements

- The local clock of Device C is set as the NTP master clock, with a clock stratum level of 2. Configure Device C to work in the NTP multicast server mode and advertise multicast NTP messages through VLAN-interface 2.
- Device A and Device D are two S4500 Ethernet switches. Configure Device A and Device D to work in the NTP multicast client mode and listen to multicast messages through their own VLAN-interface 2.

Network diagram

Figure 1-9 Network diagram for NTP multicast mode configuration



Configuration procedure

- Configure Device C.

Enter system view.

```
<DeviceC> system-view
```

Set Device C as a multicast server to send multicast messages through VLAN-interface 2.

```
[DeviceC] interface Vlan-interface 2
[DeviceC-Vlan-interface2] ntp-service multicast-server
```

- Configure Device A (perform the same configuration on Device D).

Enter system view.

```
<DeviceA> system-view
```

Set Device A as a multicast client to listen to multicast messages through VLAN-interface 2.

```
[DeviceA] interface Vlan-interface 2
[DeviceA-Vlan-interface2] ntp-service multicast-client
```

After the above configurations, Device A and Device D respectively listen to multicast messages through their own VLAN-interface 2, and Device C advertises multicast messages through VLAN-interface 2. Because Device A and Device C do not share the same network segment, Device A cannot receive multicast messages from Device C, while Device D is synchronized to Device C after receiving multicast messages from Device C.

View the NTP status of Device D after the clock synchronization.

```
[DeviceD] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^18
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
```

```
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)
```

The output information indicates that Device D is synchronized to Device C, with a clock stratum level of 3, one stratum level lower than that Device C.

View the information about the NTP sessions of Device D (you can see that a connection is established between Device D and Device C).

```
[DeviceD] display ntp-service sessions
   source         reference       stra reach poll  now offset  delay disper
**************************************************************************
[1234]3.0.1.31     127.127.1.0      2    1     64    377  26.1   199.53  9.7
note:  1  source(master),2  source(peer),3  selected,4  candidate,5  configured  Total
associations :  1
```

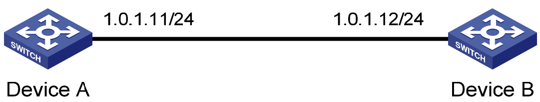
Configuring NTP Server/Client Mode with Authentication

Network requirements

- The local clock of Device A is set as the NTP master clock, with a clock stratum level of 2.
- Device B is an S4500 Ethernet switch and uses Device A as the NTP server. Device B is set to work in client mode, while Device A works in server mode automatically.
- The NTP authentication function is enabled on Device A and Device B.

Network diagram

Figure 1-10 Network diagram for NTP server/client mode with authentication configuration



Configuration procedure

- Configure Device B.

Enter system view.

```
<DeviceB> system-view
```

Enable the NTP authentication function.

```
[DeviceB] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being 42 and the key being aNiceKey.

```
[DeviceB] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key 42 as a trusted key.

```
[DeviceB] ntp-service reliable authentication-keyid 42
```

Associate the trusted key with the NTP server (Device A).

```
[DeviceB] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

After the above configurations, Device B is ready to synchronize with Device A. Because the NTP authentication function is not enabled on Device A, the clock of Device B will fail to be synchronized to that of Device A.

- To synchronize Device B, you need to perform the following configurations on Device A.

Enable the NTP authentication function.

```
<DeviceA> system-view
[DeviceA] ntp-service authentication enable
```

Configure an MD5 authentication key, with the key ID being 42 and the key being aNiceKey.

```
[DeviceA] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

Specify the key 42 as a trusted key.

```
[DeviceA] ntp-service reliable authentication-keyid 42
```

(After the above configurations, the clock of Device B can be synchronized to that of Device A.) View the status of Device B after synchronization.

```
[DeviceB] display ntp-service status
 Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequence: 100.0000 Hz
 Actual frequence: 100.1000 Hz
 Clock precision: 2^18
 Clock offset: 0.66 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Apr 2 2007 (BF422AE4.05AEA86C)
```

The output information indicates that the clock of Device B is synchronized to that of Device A, with a clock stratum level of 3, one stratum level lower than that Device A.

View the information about NTP sessions of Device B (you can see that a connection is established between Device B and Device A).

```
<DeviceB> display ntp-service sessions
       source          reference       stra reach poll  now offset  delay disper
*************************************************************************        [12345]
1.0.1.11    127.127.1.0        2   255   64    8    2.8   17.7    1.2
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

Table of Contents

1 SSH Configuration

When configuring SSH, go to these sections for information you are interested:

- SSH Overview
- SSH Server and Client
- Displaying and Maintaining SSH Configuration
- Comparison of SSH Commands with the Same Functions
- SSH Configuration Examples

SSH Overview

Introduction to SSH

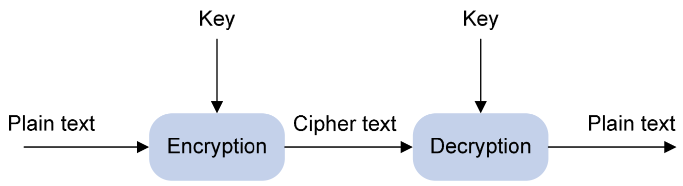
Secure Shell (SSH) is a protocol that provides secure remote login and other security services in insecure network environments, allowing for secure access to the Command Line Interface (CLI) of a switch for configuration and management. In an SSH connection, data are encrypted before being sent out and decrypted after they reach the destination. This prevents attacks such as plain text password interception. SSH also provides powerful user authentication functions that prevent attacks such as DNS and IP spoofing. Besides, SSH can also provide data compression to increase transmission speed, take the place of Telnet and provide a secure "channel" for transfers using File Transfer Protocol（FTP）.

SSH adopts the client-server model. The switch can be configured as an SSH client, an SSH server, or both at the same time. As an SSH server, the switch provides secure connections to multiple clients. As an SSH client, the switch allows the remote server to establish a secure SSH connection for remote login.

Algorithm and Key

Algorithm is a set of transformation rules for encryption and decryption. Information without being encrypted is known as plain text, while information that is encrypted is known as cipher text. Encryption and decryption are performed using a string of characters called a key, which controls the transformation between plain text and cipher text, for example, changing the plain text into cipher text or cipher text into plain text.

Figure 1-1 Encryption and decryption



There are two types of key algorithms:

- Symmetric key algorithm

The same key is used for both encryption and decryption. Supported symmetric key algorithms include DES, 3DES, and AES, which can effectively prevent data eavesdropping.

- Asymmetric key algorithm

Asymmetric key algorithm is also called public key algorithm. Both ends have their own key pair, consisting of a private key and a public key. The private key is kept secret while the public key may be distributed widely. The private key cannot be practically derived from the public key. The information encrypted with the public key/private key can be decrypted only with the corresponding private key/public key.

Asymmetric key algorithm encrypts data using the public key and decrypts the data using the private key, thus ensuring data security.

You can also use the asymmetric key algorithm for data signature. For example, user 1 adds his signature to the data using the private key, and then sends the data to user 2. User 2 verifies the signature using the public key of user 1. If the signature is correct, this means that the data originates from user 1.

Both Revest-Shamir-Adleman Algorithm (RSA) and Digital Signature Algorithm (DSA) are asymmetric key algorithms. RSA is used for data encryption and signature, whereas DSA is used for adding signature. Currently the switch supports only RSA .

Note

Symmetric key algorithms are used for encryption and decryption of the data transferred on the SSH channel while asymmetric key algorithms are used for digital signature and identity authentication.

SSH Operating Process

The session establishment between an SSH client and the SSH server involves the following five stages:

Table 1-1 Stages in establishing a session between the SSH client and server

Stages	Description
Version negotiation	SSH1 and SSH2 are supported. The two parties negotiate a version to use.
Key and algorithm negotiation	SSH supports multiple algorithms. The two parties negotiate an algorithm for communication.
Authentication	The SSH server authenticates the client in response to the client's authentication request.
Session request	This client sends a session request to the server.
Data exchange	The client and the server start to communicate with each other.

Caution

Currently, the switch supports only SSH2 Version.

Version negotiation

- The server opens port 22 to listen to connection requests from clients.
- The client sends a TCP connection request to the server. After the TCP connection is established, the server sends the first packet to the client, which includes a version identification string in the format of "SSH-<primary protocol version number>.<secondary protocol version number>-<software version number>". The primary and secondary protocol version numbers constitute the protocol version number, while the software version number is used for debugging.
- The client receives and resolves the packet. If the protocol version of the server is lower but supportable, the client uses the protocol version of the server; otherwise, the client uses its own protocol version.
- The client sends to the server a packet that contains the number of the protocol version it decides to use. The server compares the version carried in the packet with that of its own to determine whether it can cooperate with the client.
- If the negotiation is successful, the server and the client go on to the key and algorithm negotiation. If not, the server breaks the TCP connection.

Note

All the packets above are transferred in plain text.

Key negotiation

- The server and the client send algorithm negotiation packets to each other, which contain public key algorithm lists supported by the server and the client, encrypted algorithm list, message authentication code (MAC) algorithm list, and compressed algorithm list.
- The server and the client calculate the final algorithm according to the algorithm lists supported.
- The server and the client generate the session key and session ID based on the Diffie-Hellman (DH) exchange algorithm and the host key pair.
- Then, the server and the client get the same session key and use it for data encryption and decryption to secure data communication.

Authentication negotiation

The negotiation steps are as follows:

- The client sends an authentication request to the server. The authentication request contains username, authentication type, and authentication-related information. For example, if the authentication type is **password**, the content is the password.

- The server starts to authenticate the user. If authentication fails, the server sends an authentication failure message to the client, which contains the list of methods used for a new authentication process.
- The client selects an authentication type from the method list to perform authentication again.
- The above process repeats until the authentication succeeds, or the connection is torn down when the authentication times reach the upper limit.

SSH provides two authentication methods: password authentication and publickey authentication.

- In password authentication, the client encrypts the username and password, encapsulates them into a password authentication request, and sends the request to the server. Upon receiving the request, the server decrypts the username and password, compares them with those it maintains, and then informs the client of the authentication result.
- The publickey authentication method authenticates clients using digital signatures. Currently, the device supports only RSA to implement digital signatures. The client sends to the server a publickey authentication request containing its user name, public key and algorithm. The server verifies the public key. If the public key is invalid, the authentication fails; otherwise, the server generates a digital signature to authenticate the client, and then sends back a message to inform the success or failure of the authentication.

Session request

After passing authentication, the client sends a session request to the server, while the server listens to and processes the request from the client. If the client passes authentication, the server sends back to the client an SSH_SMSG_SUCCESS packet and goes on to the interactive session stage with the client. Otherwise, the server sends back to the client an SSH_SMSG_FAILURE packet, indicating that the processing fails or it cannot resolve the request. The client sends a session request to the server, which processes the request and establishes a session.

Data exchange

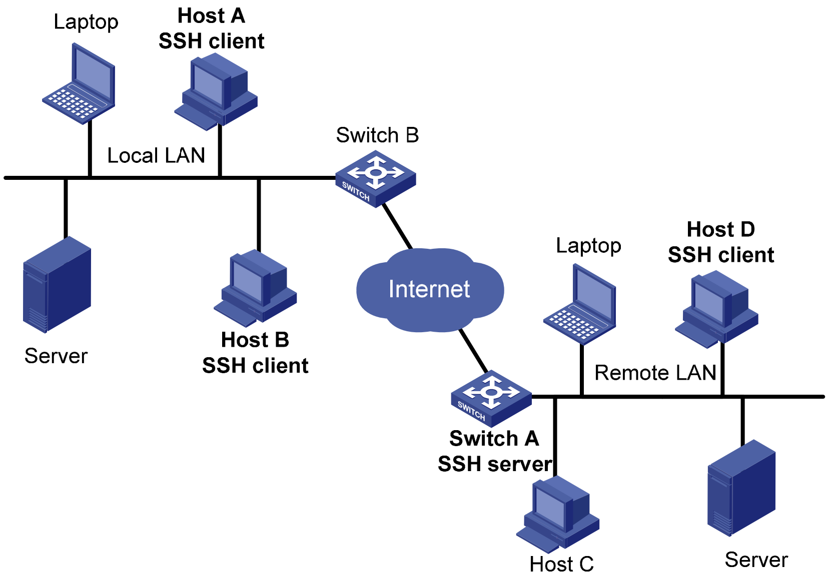
In this stage, the server and the client exchanges data in this way:

- The client encrypts and sends the command to be executed to the server.
- The server decrypts and executes the command, and then encrypts and sends the result to the client.
- The client decrypts and displays the result on the terminal.

SSH Server and Client

To use SSH for secure login to a switch from a device, the switch must be configured as an SSH server and the device must be configured as an SSH client. As shown in Figure 1-2, Host A, Host B, and Host D are configured as SSH clients to securely access the Switch A, which is acting as the SSH server.

Figure 1-2 Network diagram for SSH connections



Configure the devices accordingly This document describes two cases:

- The 3Com switch acts as the SSH server to cooperate with software that supports the SSH client functions.
- The 3Com switch acts as the SSH server to cooperate with another 3Com switch that acts as an SSH client.

Complete the following tasks to configure the SSH server and clients:

Server	Client	Server side configuration	Client side configuration
An 3Com switch	Software that supports the SSH client functions	Configuring the SSH Server	Configuring an SSH Client that Runs SSH Client Software
An 3Com switch	Another 3Com switch	Configuring the SSH Server	Configuring an SSH Client Assumed by an SSH2-Capable Switch

Note

An SSH server forms a secure connection with each SSH client. The following describe steps for configuring an SSH client and an SSH server to form an SSH connection in between. If multiple SSH servers need to form connections with multiple SSH clients, configure each client and each server accordingly.

Configuring the SSH Server

The session establishment between an SSH client and the SSH server involves five stages. Similarly, SSH server configuration involves five aspects, as shown in the following table.

Complete the following tasks to configure the SSH server:

Task		Remarks
Preparation	Configuring the User Interfaces for SSH Clients	Required
	Configuring the SSH Management Functions	Optional
Key	Configuring Key Pairs	Required
Authentication	Creating an SSH User and Specifying an Authentication Type	Required
Authorization	Specifying a Service Type for an SSH User	Optional By default, an SSH user can use the service type of **stelnet**.
Data exchange	Configuring the Public Key of a Client on the Server	• Not necessary when the authentication mode is **password**. • Required when the authentication mode is **publickey**.
	Assigning a Public Key to an SSH User	• Not necessary when the authentication mode is **password**. • Required when the authentication mode is **publickey**.
	Exporting the Host Public Key	Optional If a client does not support first-time authentication, you need to export the server's public key and configure the key on the client.

Note

The SSH server needs to cooperate with an SSH client to complete the interactions between them. For SSH client configuration, refer to Configuring the SSH Client.

Configuring the User Interfaces for SSH Clients

An SSH client will access the device through a terminal "VTY" user interface. Therefore, you need to configure the device user interface to accept SSH clients and allow SSH login. Note that the configuration takes effect at the next login.

Follow these steps to configure the device user interface for SSH clients:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter user interface view of one or more user interfaces	**user-interface vty** *first-number* [*last-number*]	—
Configure the authentication mode as scheme	**authentication-mode scheme** [**command-authorization**]	Required By default, the user interface authentication mode is password.

To do...	Use the command...	Remarks
Specify the supported protocol(s)	**protocol inbound** { **all** |**ssh** }	Optional By default, both Telnet and SSH are supported.

Caution

- If you have configured a user interface to support SSH protocol, you must configure AAA authentication for the user interface by using the **authentication-mode scheme** command to ensure successful login.
- On a user interface, if the **authentication-mode password** or **authentication-mode none** command has been executed, the **protocol inbound ssh** command is not available. Similarly, if the **protocol inbound ssh** command has been executed, the **authentication-mode password** and **authentication-mode none** commands are not available.

Configuring the SSH Management Functions

The SSH server provides a number of management functions to prevent illegal operations such as malicious password guess, guaranteeing the security of SSH connections. You can specify the IP address or the interface corresponding to the IP address for the SSH server to provide SSH access services for clients. In this way, the SSH client accesses the SSH server only using the specified IP address. This increases the service manageability when the SSH server has multiple interfaces and IP addresses.

Follow these steps to configure SSH management functions:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Set the SSH authentication timeout time	**ssh server timeout** *seconds*	Optional By default, the SSH authentication timeout time is 60 seconds.
Set the number of SSH authentication retry attempts	**ssh server authentication-retries** *times*	Optional By default, the number of SSH authentication retry attempts is 3.
Configure a login header	**header shell** *text*	Optional By default, no login header is configured.
Specify a source IP address for the SSH server	**ssh-server source-ip** *ip-address*	Optional By default, no source IP address is configured.
Specify a source interface for the SSH server	**ssh-server source-interface** *interface-type interface-number*	Optional By default, no source interface is configured.

Caution

- You can configure a login header only when the service type is **stelnet**. For configuration of service types, refer to Specifying a Service Type for an SSH User.
- For details of the **header** command, refer to the corresponding section in *Login Command*.

Configuring Key Pairs

The SSH server's key pairs are for generating session keys and for SSH clients to authenticate the server. The SSH client's key pairs are for the SSH server to authenticate the SSH clients in publickey authentication mode. RSA key pair are only supported.

Generating key pairs

When generating a key pair, you will be prompted to enter the key length in bits, which is between 512 and 2048. The default length is 1024. If the key pair already exists, the system will ask whether to overwrite it.

Follow these steps to create key pairs:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Generate an RSA key pairs	**public-key local create rsa**	Required By default, no key pairs are generated.

Note

- The command for generating a key pair can survive a reboot. You only need to configure it once.
- It takes more time to encrypt and decrypt data with a longer key, which, however, ensures higher security. Therefore, specify the length of the key pair accordingly.
- For a fabric made up of multiple devices, you need to create the key pairs on the device to ensure that all devices in the fabric have the same local RSA key pairs.
- Some third-party software, for example, WinSCP, requires that the modulo of a public key must be greater than or equal to 768. Therefore, a local key pair of more than 768 bits is recommended.

Destroying key pairs

The RSA key may be exposed, and you may want to destroy the keys and generate new ones.

Follow these steps to destroy key pairs:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Destroy the RSA key pair	**public-key local destroy rsa**	Optional

Creating an SSH User and Specifying an Authentication Type

This task is to create an SSH user and specify an authentication type. Specifying an authentication type for a new user is a must to get the user login.

An SSH user is represented as a set of user attributes on the SSH server. This set is uniquely identified with the SSH username. When a user logs in to the SSH server from the SSH client, a username is required so that the server can looks up the database for matching the username. If a match is found, it authenticates the user using the authentication mode specified in the attribute set. If not, it tears down the connection.

To prevent illegal users from logging in to the device, SSH supports the authentication modes of password, publickey, and password-publickey.

- Password authentication

SSH uses the authentication function of AAA to authenticate the password of the user that is logging in. Based on the AAA authentication scheme, password authentication can be done locally or remotely. For local authentication, the SSH server saves the user information and implements the authentication. For remote authentication, the user information is saved on an authentication server (such as a RADIUS server) and authentication is implemented through the cooperation of the SSH server and the authentication server. For AAA details, refer to *AAA Operation*.

- Publickey authentication

Publickey authentication provides more secure SSH connections than password authentication does. At present, the device supports RSA for publickey authentication. After configuration, authentication is implemented automatically without asking you to enter the password. In this mode, you need to create a key pair on each client, and configure each client's public key on the server. This may be complicated when multiple SSH clients want to access one SSH server in the network.

- Password-publickey authentication

An SSH user must pass both types of authentication before logging in. In this mode, you do not need to create a key pair on each client. You can configure the clients to use the same key pair that is created on one client for publickey authentication. With the AAA function in password authentication, the level of commands available to a logged-in SSH user is determined by the AAA scheme..

Follow these steps to configure an SSH user and specify an authentication type for the user:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Specify the default authentication type for all SSH users	**ssh authentication-type default** { **all** | **password** | **password-publickey** | **publickey** }	Use either command. By default, no SSH user is created and no authentication type is specified. Note that: If both commands
	ssh user *username*	

To do...	Use the command...	Remarks
Create an SSH user, and specify an authentication type for it	**ssh user** *username* **authentication-type** { **all** | **password** | **password-publickey** | **publickey** }	are used and different authentication types are specified, the authentication type specified with the **ssh user authentication-type** command takes precedence.

Caution

- For **password** authentication type, the *username* argument must be consistent with the valid user name defined in AAA; for publickey authentication, the *username* argument is the SSH local user name, so that there is no need to configure a local user in AAA.
- If the default authentication type for SSH users is **password** and local AAA authentication is adopted, you need not use the **ssh user** command to create an SSH user. Instead, you can use the **local-user** command to create a user name and its password and then set the service type of the user to SSH.
- If the default authentication type for SSH users is password and remote authentication (RADIUS authentication, for example) is adopted, you need not use the **ssh user** command to create an SSH user, because it is created on the remote server. And the user can use its username and password configured on the remote server to access the network.
- Under the **publickey** authentication mode, the level of commands available to a logged-in SSH user can be configured using the **user privilege level** command on the server, and all the users with this authentication mode will enjoy this level.
- Under the **password** or **password-publickey** authentication mode, the level of commands available to a logged-in SSH user is determined by the AAA scheme. Meanwhile, for different users, the available levels of commands are also different.
- Under the **all** authentication mode, the level of commands available to a logged-in SSH user is determined by the actual authentication method used for the user.

Specifying a Service Type for an SSH User on the Server

At present, the switch supports two service types for SSH: stelnet (secure Telnet) and SFTP.

- The secure Telnet service is a basic application of SSH protocol. It uses the secure channel of SSH to provide remote login.
- The SFTP service is an extended application of SSH protocol. It uses the secure channel of SSH to perform remote FTP operations.

Follow these steps to specify the service type for an SSH user:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Specify a service type for an SSH user	**ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }	Required By default, an SSH user can use the service type of **stelnet**.

Caution

If the **ssh user service-type** command is executed with a username that does not exist, the system will automatically create the SSH user. However, the user cannot log in unless you specify an authentication type for it.

Configuring the Public Key of a Client on the Server

Note

This configuration is not necessary if the **password** authentication mode is configured for SSH users.

With the **publickey** authentication mode configured for an SSH client, you must configure the client's RSA host public key on the server for authentication.

You can manually configure the public key or import it from a public key file. In the former case, you can manually copy the client's public key to the server. In the latter case, the system automatically converts the format of the public key generated by the client to complete the configuration on the server, but the client's public key should be transferred from the client to the server beforehand through FTP/TFTP.

Follow these steps to configure the public key of a client manually:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter public key view	**public-key peer** *keyname*	Required
Enter public key edit view	**public-key-code begin**	—
Configure a public key for the client	Enter the content of the public key	When you input the key, spaces are allowed between the characters you input (because the system can remove the spaces automatically); you can also press **Enter** to continue your input at the next line. But the key you input should be a hexadecimal digit string coded in the public key format.
Return to public key view from public key edit view	**public-key-code end**	—
Exit public key view and return to system view	**peer-public-key end**	—

Follow these steps to import the public key from a public key file:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Import the public key from a public key file	**public-key peer** *keyname* **import sshkey** *filename*	Required

Assigning a Public Key to an SSH User

Caution

This configuration task is unnecessary if the SSH user's authentication mode is **password**.

For the **publickey** authentication mode, you must specify the client's public key on the server for authentication.

Follow these steps to assign a public key for an SSH user:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Assign a public key to an SSH user	**ssh user** *username* **assign publickey** *keyname*	Required If you issue this command multiple times, the last command overrides the previous ones.

Exporting the Host Public Key to a File

In tasks of Configuring the Public Key of a Client on the Server or Configuring whether first-time authentication is supported, an SSH client's or an SSH server's host public key can be imported from a public key file. This task allows you to export the host public key to a file on the client or server device with key pairs generated.

Follow these steps to export the RSA host public key:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Export the RSA host public key to a specified file	**public-key local export rsa** { **openssh** | **ssh1** | **ssh2** } [*filename*]	Required

Note

With the *filename* argument specified, you can export the RSA host public key to a file so that you can configure the key at a remote end by importing the file. If the *filename* argument is not specified, this command displays the host public key information on the screen in a specified format.

Configuring the SSH Client

The configurations required on the SSH client are related to the authentication mode that the SSH server uses. In addition, if an SSH client does not support first-time authentication, you need to configure the public key of the server on the client, so that the client can authenticate the server.

SSH Client Configuration Task List

Complete the following tasks to configure the SSH client:

Scenario	SSH client configuration task	
	For a client running SSH client software	For a client assumed by an SSH2-capable switch
The authentication mode is **password**	Configuring an SSH Client that Runs SSH Client Software	Configuring an SSH Client Assumed by an SSH2-Capable Switch
The authentication mode is **publickey**	Configuring an SSH Client that Runs SSH Client Software	Configuring an SSH Client Assumed by an SSH2-Capable Switch
Whether first-authentication is supported	—	Configuring an SSH Client Assumed by an SSH2-Capable Switch

Configuring an SSH Client that Runs SSH Client Software

A variety of SSH client software are available, such as PuTTY and OpenSSH. For an SSH client to establish a connection with an SSH server, use the following commands:

Complete the following tasks to configure an SSH client that runs SSH client software:

Task	Remarks
Generating a client key	Required for **publickey** authentication; unnecessary for **password** authentication
Specifying the IP address of the Server	Required
Selecting a protocol for remote connection	Required
Selecting an SSH version	Required
Opening an SSH connection with password authentication	Required for **password** authentication; unnecessary for **publickey** authentication

Task	Remarks
Opening an SSH connection with publickey authentication	Required for **publickey** authentication; unnecessary for **password** authentication

Note

- For putty, it is recommended to use PuTTY release 0.53; PuTTY release 0.58 is also supported. For OpenSSH, it is recommended to use OpenSSH_3.1p1; OpenSSH_4.2p1 is also supported. Any other version or other client, please be careful to use.
- Selecting the protocol for remote connection as SSH. Usually, a client can use a variety of remote connection protocols, such as Telnet, Rlogin, and SSH. To establish an SSH connection, you must select SSH
- Selecting the SSH version. Since the device supports only SSH2.0 now, select 2.0 for the client.
- Specifying the private key file. On the server, if public key authentication is enabled for an SSH user and a public key is set for the user, the private key file corresponding to the public key must be specified on the client. RSA key pairs are generated by a tool of the client software.

The following takes the client software of PuTTY Version 0.58 as an example to illustrate how to configure the SSH client:

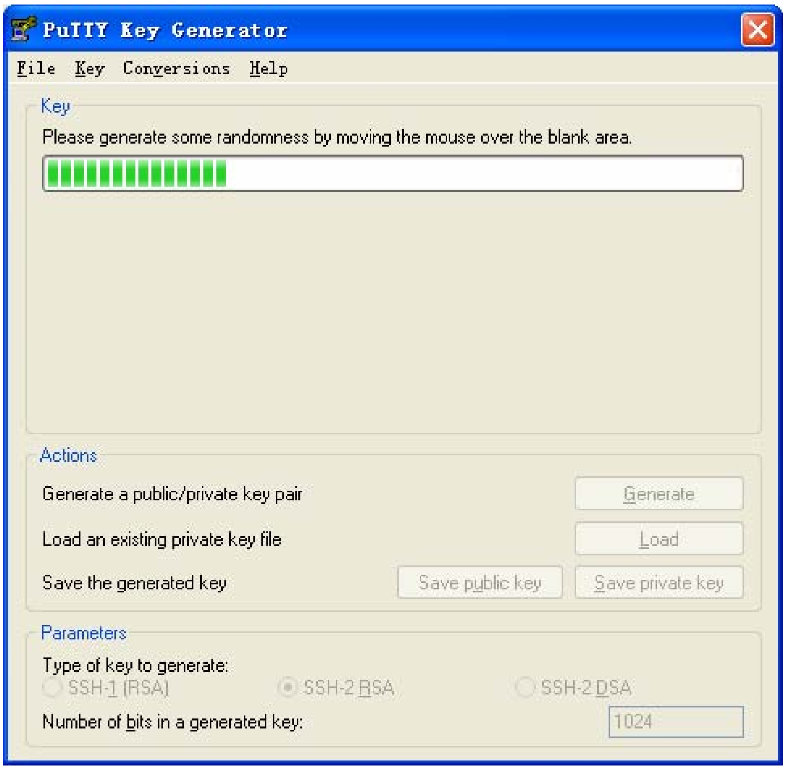
Generating a client key

To generate a client key, run PuTTYGen.exe, and select from the **Parameters** area the type of key you want to generate, either SSH-2 RSA , then click **Generate**.

Figure 1-3 Generate a client key (1)

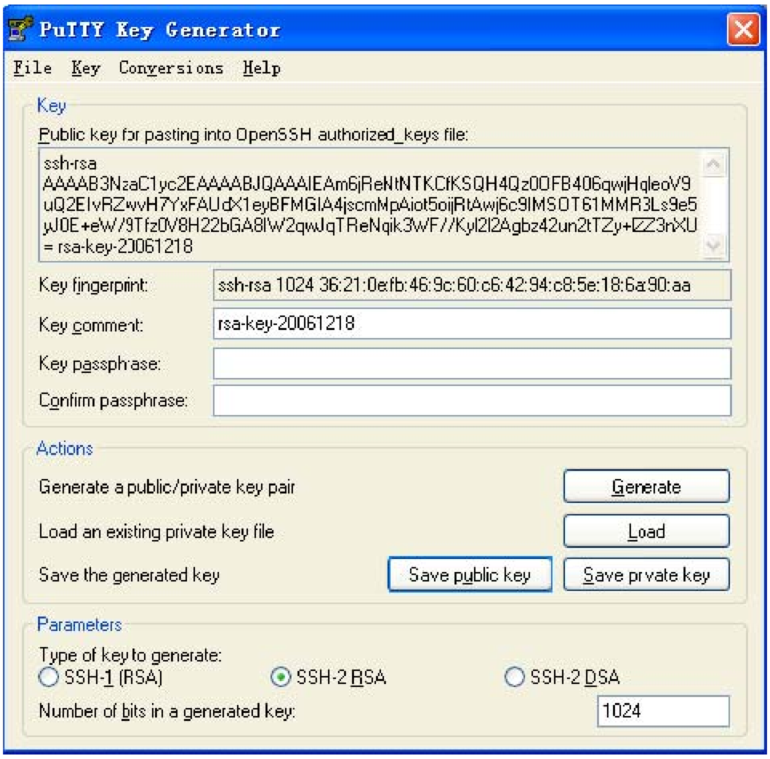
Note that while generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar in the blue box of shown in Figure 1-4. Otherwise, the process bar stops moving and the key pair generating process is stopped.

Figure 1-4 Generate the client keys (2)



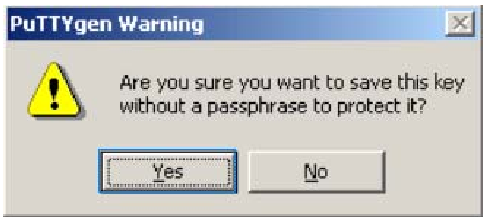
After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (**public** in this case) to save the public key.

Figure 1-5 Generate the client keys (3)



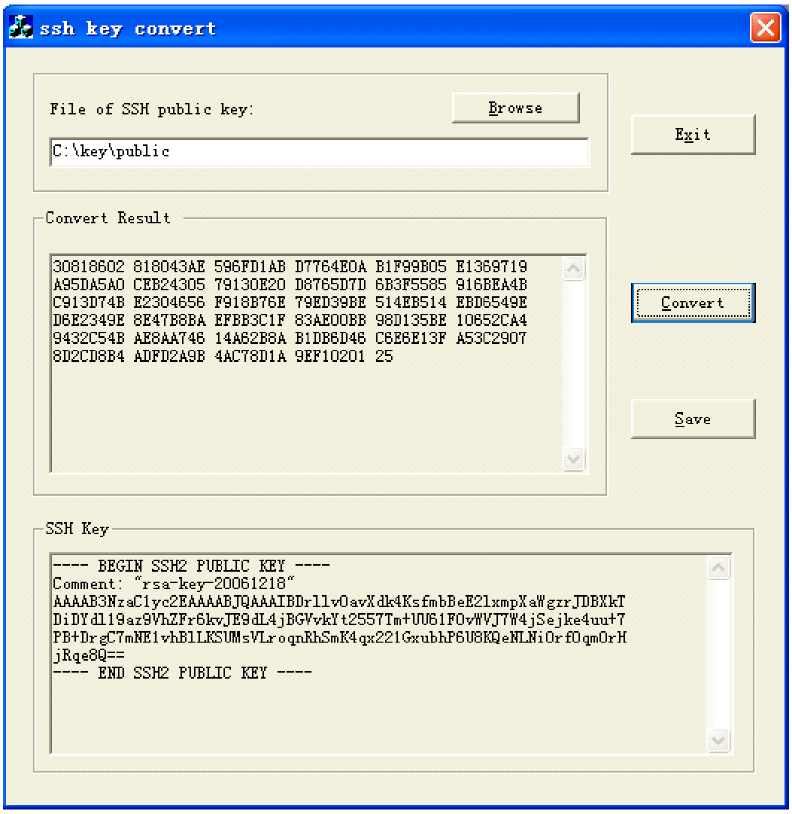
Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any precaution. Click **Yes** and enter the name of the file for saving the private key ("private" in this case) to save the private key.

Figure 1-6 Generate the client keys (4)



To generate RSA public key in PKCS format, run SSHKEY.exe, click **Browse** and select the public key file, and then click **Convert**.

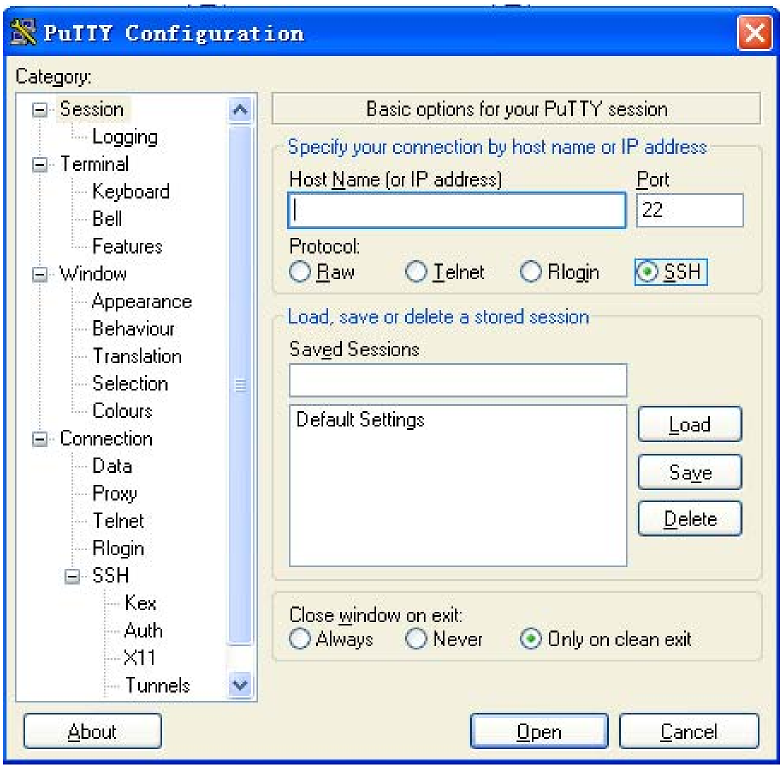
Figure 1-7 Generate the client keys (5)



Specifying the IP address of the Server

Launch PuTTY.exe. The following window appears.

Figure 1-8 SSH client configuration interface 1



In the **Host Name (or IP address)** text box, enter the IP address of the server. Note that there must be a route available between the IP address of the server and the client.

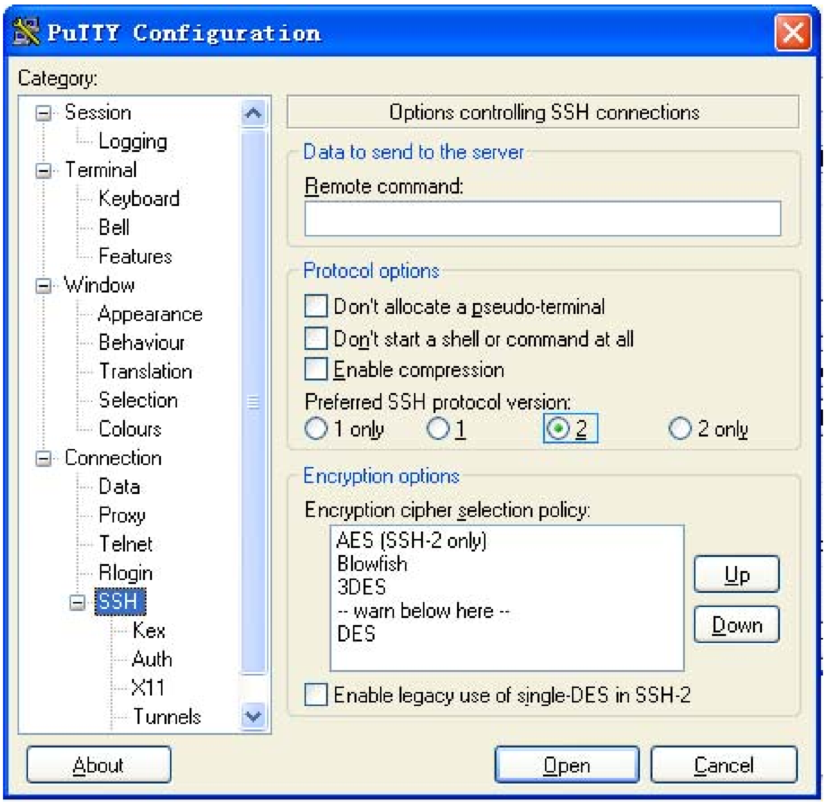
Selecting a protocol for remote connection

As shown in Figure 1-8, select **SSH** under **Protocol**.

Selecting an SSH version

From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 1-9 appears.

Figure 1-9 SSH client configuration interface 2



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

Note

Some SSH client software, for example, Tectia client software, supports the DES algorithm only when the ssh1 version is selected. The PuTTY client software supports DES algorithm negotiation ssh2.

Opening an SSH connection with password authentication

From the window shown in Figure 1-9, click **Open**. If the connection is normal, you will be prompted to enter the username and password.

Enter the username and password to establish an SSH connection.

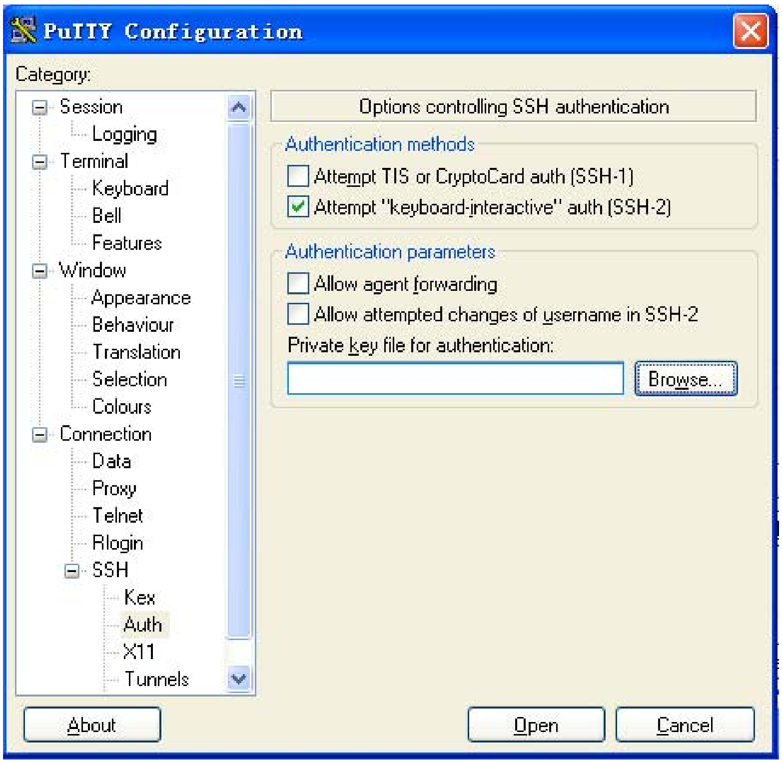
To log out, enter the quit command.

Opening an SSH connection with publickey authentication

If a user needs to be authenticated with a public key, the corresponding private key file must be specified. A private key file is not required for password-only authentication.

From the category on the left of the window, select **Connection**/**SSH**/**Auth**. The following window appears.

Figure 1-10 SSH client configuration interface 3



Click **Browse…** to bring up the file selection window, navigate to the private key file and click **Open**. If the connection is normal, a user will be prompted for a username. Once passing the authentication, the user can log in to the server.

Configuring an SSH Client Assumed by an SSH2-Capable Switch

Complete the following tasks to configure an SSH client that is assumed by an SSH2-capable switch:

Task	Remarks
Configuring the SSH client for publickey authentication	Required for **publickey** authentication; unnecessary for **password** authentication
Configuring whether first-time authentication is supported	Optional
Specifying a source IP address/interface for the SSH client	Optional
Establishing the connection between the SSH client and server	Required

Configuring the SSH client for publickey authentication

When the authentication mode is **publickey**, you need to configure the RSA public key of the client on the server:

- To generate a key pair on the client, refer to Configuring Key Pairs.
- To export the RSA public key of the client, refer to Exporting the Host Public Key.
- To configure the public key of a client on the server, refer to Configuring the Public Key of a Client on the Server.

Configuring whether first-time authentication is supported

When the device connects to the SSH server as an SSH client, you can configure whether the device supports first-time authentication.

- With first-time authentication enabled, an SSH client that is not configured with the server host public key can continue accessing the server when it accesses the server for the first time, and it will save the host public key on the client for use in subsequent authentications.
- With first-time authentication disabled, an SSH client that is not configured with the server host public key will be denied of access to the server. To access the server, a user must configure in advance the server host public key locally and specify the public key name for authentication.

Follow these steps to enable the device to support first-time authentication:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable the device to support first-time authentication	**ssh client first-time enable**	Optional By default, the client is enabled to run first-time authentication.

Follow these steps to disable first-time authentication support:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Disable first-time authentication support	**undo ssh client first-time**	Required By default, the client is enabled to run first-time authentication.
Configure server public key	Refer to Configuring the Public Key of a Client on the Server	Required The method of configuring server public key on the client is similar to that of configuring client public key on the server.
Specify the host key name of the server	**ssh client** { *server-ip* | *server-name* } **assign publickey** *keyname*	Required

Note

With first-time authentication enabled, an SSH client that is not configured with the SSH server's host public key saves the host public key sent by the server without authenticating the server. Attackers may exploit the vulnerability to initiate man-in-middle attacks by acting as an SSH server. Therefore, it is recommended to disable first-time authentication unless you are sure that the SSH server is reliable.

Specifying a source IP address/interface for the SSH client

You can configure a souce IP address or the souce IP address by specifying the corresponding interface for the client to use to access the SSH server. This improves the service manageability when the SSH client has multiple IP addresses and interfaces

Follow these steps to specify a source IP address/interface for the SSH client:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Specify a source IP address for the SSH client	**ssh2 source-ip** *ip-address*	Optional By default, no source IP address is configured.
Specify a source interface for the SSH client	**ssh2 source-interface** *interface-type interface-number*	Optional By default, no source interface is configured.

Establishing the connection between the SSH client and server

The client's method of establishing an SSH connection to the SSH server varies with authentication types.

Follow these steps to establish an SSH connection:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Start the client to establish a connection with an SSH server	**ssh2** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **3des** | **des** | **aes128** } | **prefer_stoc_cipher** { **3des** | **des** | **aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	Required In this command, you can also specify the preferred key exchange algorithm, encryption algorithms and HMAC algorithms between the server and client. HMAC: Hash-based message authentication code. Support for the 3des keyword depends on the number of encryption bits of the software version. The 168-bit version supports this keyword, while the 56-bit version does not.

Displaying and Maintaining SSH Configuration

To do...	Use the command...	Remarks
Display the public key information of the current switch's key pairs	**display public-key local rsa public**	Available in any view
Display information about locally saved public keys of SSH peers	**display public-key peer** [**brief** | **name** *pubkey-name*]	
Display information about SSH status and about sessions of active connections with SSH clients	**display ssh server** { **session** | **status** }	

To do...	Use the command...	Remarks
Display information about all SSH users	**display ssh user-information** [*username*]	
Display the current source IP address or the IP address of the source interface specified for the SSH server.	**display ssh-server source-ip**	
Display the mappings between host public keys and SSH servers saved on a client	**display ssh server-info**	
Display the current source IP address or the IP address of the source interface specified for the SSH Client.	**display ssh2 source-ip**	

Comparison of SSH Commands with the Same Functions

After some SSH configuration commands are changed. For the sake of SSH configuration compatibility, the original commands are still supported. Table 1-2 lists both the original commands and current commands.

Table 1-2 List of SSH configuration commands with the same functions

Operation	Original commands	Current commands
Display local RSA public keys	**display rsa local-key-pair public**	**display public-key local rsa public**
Display information about the peer RSA public keys	**display rsa peer-public-key** [**brief** | **name** *keyname*]	**display public-key peer** [**brief** | **name** *pubkey-name*]
Generate RSA key pairs	**rsa local-key-pair create**	**public-key local create rsa**
Destroy RSA key pairs	**rsa local-key-pair destroy**	**public-key local destroy rsa**
Enter public key view	**rsa peer-public-key** *keyname*	**public-key peer** *keyname*
Import RSA public key from public key file	**rsa peer-public-key** *keyname* **import sshkey** *filename*	**public-key peer** *keyname* **import sshkey** *filename*
Specify publickey authentication as the default authentication type for all SSH clients	**ssh authentication-type default rsa**	**ssh authentication-type default publickey**
Specify on the client the host public key of the server to be connected	**ssh client** { *server-ip* | *server-name* } **assign rsa-key** *keyname*	**ssh client** { *server-ip* | *server-name* } **assign publickey** *keyname*
Assign a public key to an SSH user	**ssh user** *username* **assign rsa-key** *keyname*	**ssh user** *username* **assign publickey** *keyname*
Create an SSH user and specify publickey authentication as its authentication type	**ssh user** *username* **authentication-type rsa**	**ssh user** *username* **authentication-type publickey**

Note

The results of the **display rsa local-key-pair public** command or the public key converted with the SSHKEY tool contains no information such as the authentication type, so they cannot be directly used as parameters in the **public-key peer** command. For the same reason, neither can the results of the **display public-key local rsa public** command be used in the **rsa peer-public-key** command directly.

SSH Configuration Examples

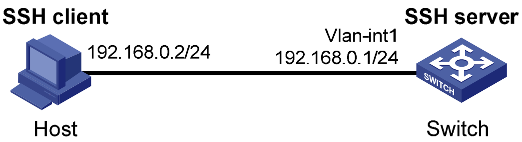
When Switch Acts as Server for Local Password Authentication

Network requirements

As shown in Figure 1-11, establish an SSH connection between the host (SSH Client) and the switch (SSH Server) for secure data exchange. The host runs SSH2.0 client software. Password authentication is required.

Network diagram

Figure 1-11 Switch acts as server for local password authentication



Configuration procedure

- Configure the SSH server

Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[Switch-Vlan-interface1] quit
```

Caution

Generating the RSA key pair on the server is prerequisite to SSH login.

Generate RSA key pair.

```
[Switch] public-key local create rsa
```

Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
```

```
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

Create local client **client001**, and set the authentication password to **abc**, protocol type to SSH, and command privilege level to 3 for the client.

```
[Switch] local-user client001
[Switch-luser-client001] password simple abc
[Switch-luser-client001] service-type ssh level 3
[Switch-luser-client001] quit
```

Specify the authentication method of user client001 as password.

```
[Switch] ssh user client001 authentication-type password
```

- Configure the SSH client

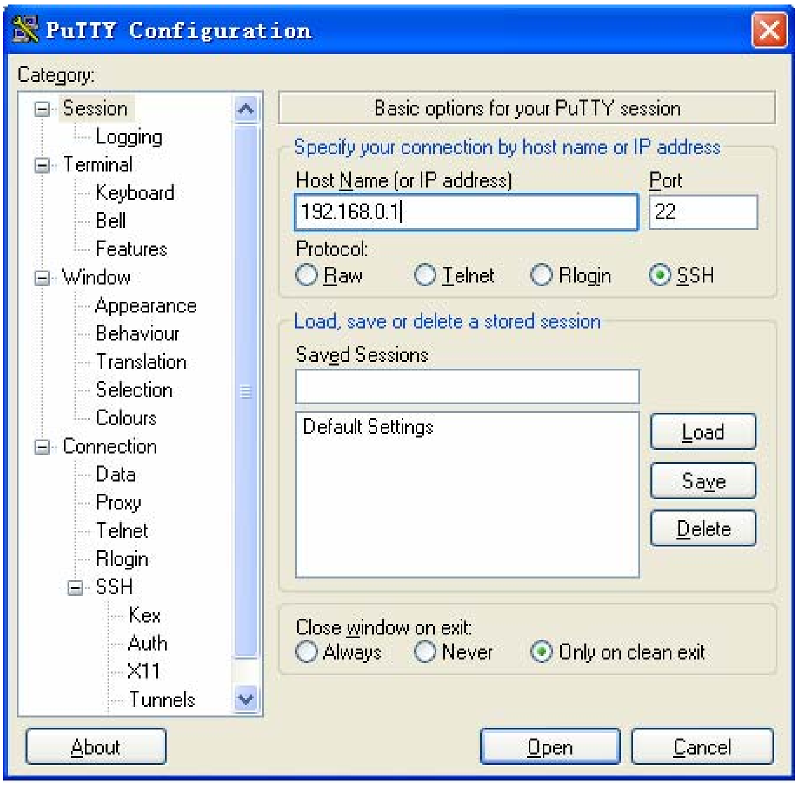
Configure an IP address (192.168.0.2 in this case) for the SSH client. This IP address and that of the VLAN interface on the switch must be in the same network segment.

Configure the SSH client software to establish a connection to the SSH server.

Take SSH client software **Putty** (version 0.58) as an example:

1) Run PuTTY.exe to enter the following configuration interface.

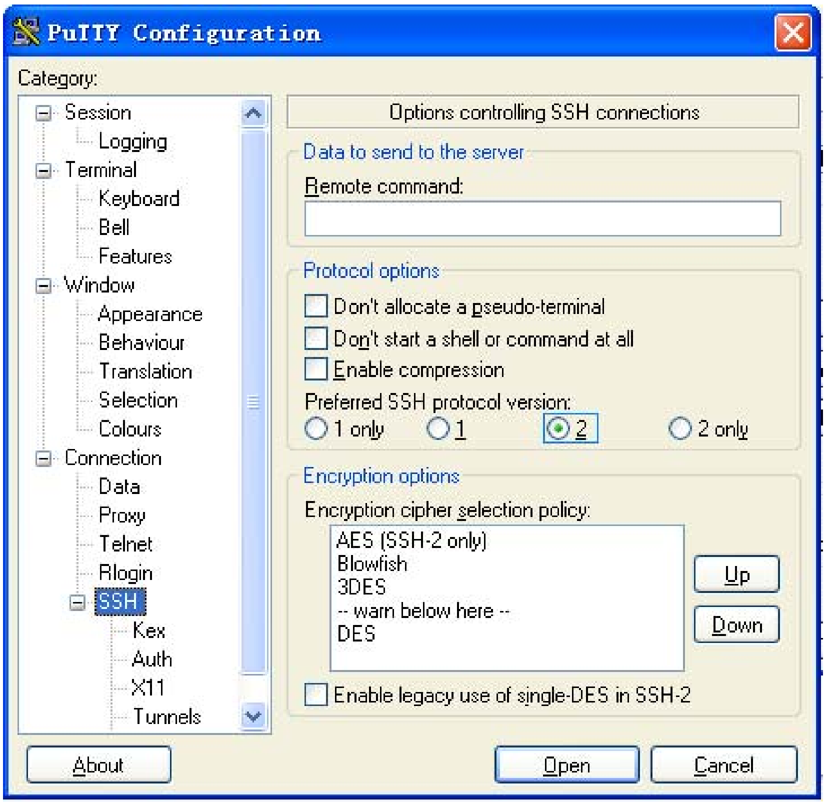
Figure 1-12 SSH client configuration interface (1)



In the **Host Name (or IP address)** text box, enter the IP address of the SSH server.

2) From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 1-13 appears.

Figure 1-13 SSH client configuration interface (2)



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

3) As shown in Figure 1-13, click **Open**. If the connection is normal, you will be prompted to enter the user name **client001** and password **abc**. Once authentication succeeds, you will log in to the server.

1.1.1 When Switch Acts as Server for Password and RADIUS Authentication

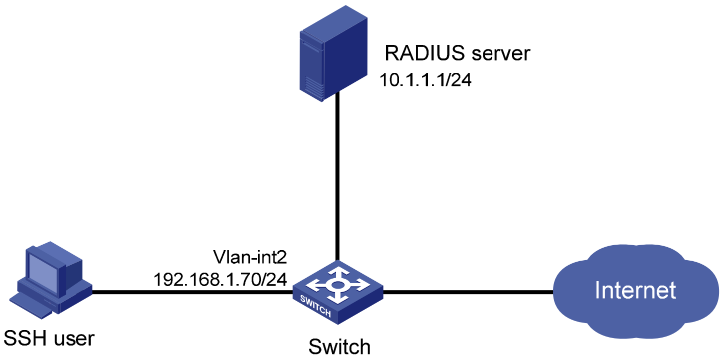
Network requirements

As shown in Figure 1-14, an SSH connection is required between the host (SSH client) and the switch (SSH server) for secure data exchange. Password and RADIUS authentication is required.

- The host runs SSH2.0 client software to establish a local connection with the switch.
- The switch cooperates with a RADIUS server to authenticate SSH users.

Network diagram

Figure 1-14 Switch acts as server for password and RADIUS authentication



Configuration procedure

1) Configure the RADIUS server

Note

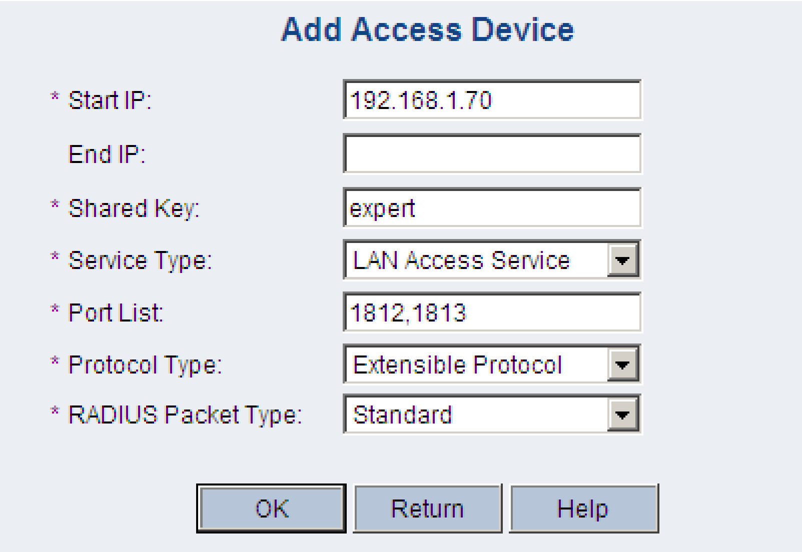
This document takes CAMS Version 2.10 as an example to show the basic RADIUS server configurations required.

Add an access device.

Log in to the CAMS management platform and select **System Management** > **System Configuration** from the navigation tree. In the **System Configuration** page, click **Modify** of the **Access Device** item, and then click **Add** to enter the **Add Access Device** page and perform the following configurations:

- Specify the IP address of the switch as 192.168.1.70.
- Set both the shared keys for authentication and accounting packets to **expert**.
- Select **LAN Access Service** as the service type.
- Specify the ports for authentication and accounting as 1812 and 1813 respectively.
- Select **Extensible Protocol** as the protocol type.
- Select **Standard** as the RADIUS packet type.

Figure 1-15 Add an access device

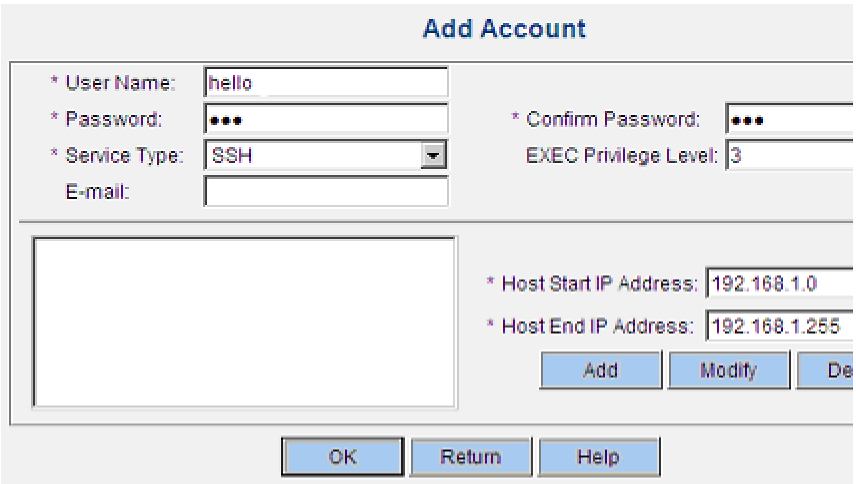


Add a user account for device management.

From the navigation tree, select **User Management** > **User for Device Management**, and then in the right pane, click **Add** to enter the **Add Account** page and perform the following configurations:

- Add a user named **hello**, and specify the password.
- Select **SSH** as the service type.
- Specify the IP address range of the hosts to be managed.

Figure 1-16 Add an account for device management



2) Configure the SSH server

Create a VLAN interface on the switch and assign it an IP address. This address will be used as the IP address of the SSH server for SSH connections.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

Caution

Generating the RSA key pair on the server is prerequisite to SSH login.

Generate RSA key pairs.

```
[Switch] public-key local create rsa
```

Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

Configure the RADIUS scheme.

```
[Switch] radius scheme rad
[Switch-radius-rad] accounting optional
[Switch-radius-rad] primary authentication 10.1.1.1 1812
[Switch-radius-rad] key authentication expert
[Switch-radius-rad] server-type extended
[Switch-radius-rad] user-name-format without-domain
[Switch-radius-rad] quit
```

Apply the scheme to the ISP domain.

```
[Switch] domain bbb
[Switch-isp-bbb] scheme radius-scheme rad
[Switch-isp-bbb] quit
```

Configure an SSH user, specifying the switch to perform password authentication for the user.

```
[Switch] ssh user hello authentication-type password
```

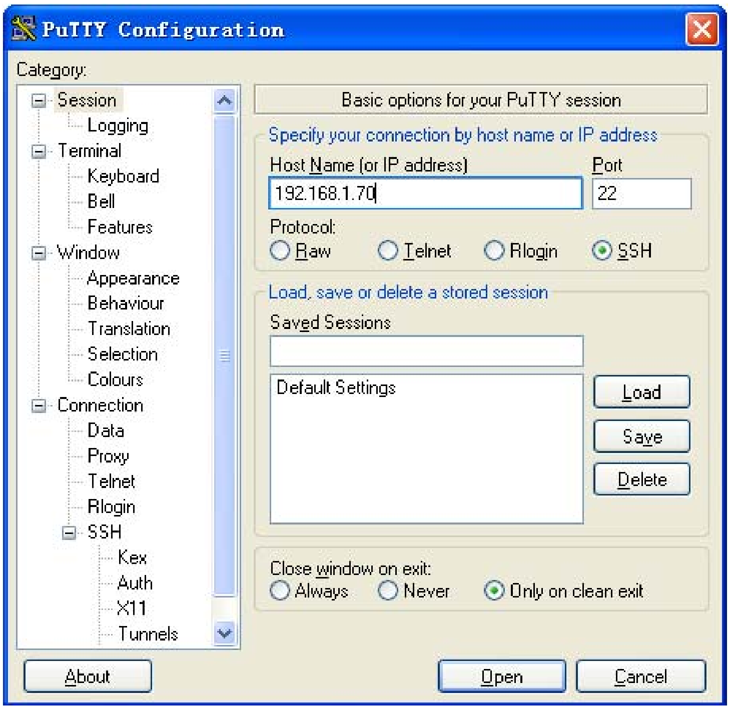
3) Configure the SSH client

Configure an IP address (192.168.1.1 in this case) for the SSH client. This IP address and that of the VLAN interface on the switch must be in the same network segment.

Configure the SSH client software to establish a connection to the SSH server. Take SSH client software Putty Version 0.58 as an example:

- Run PuTTY.exe to enter the following configuration interface.

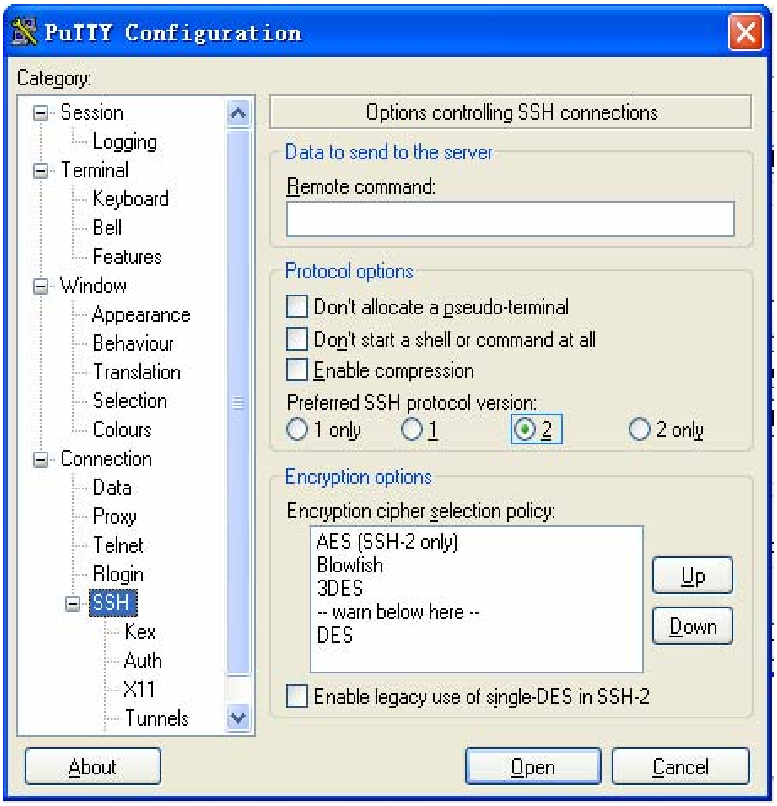
Figure 1-17 SSH client configuration interface (1)



In the **Host Name (or IP address)** text box, enter the IP address of the SSH server.

- From the category on the left pane of the window, select **Connection** > **SSH**. The window as shown in Figure 1-18 appears.

Figure 1-18 SSH client configuration interface (2)



Under **Protocol options**, select **2** from **Preferred SSH protocol version**. Then, click **Open**. If the connection is normal, you will be prompted to enter the user name **hello** and the password. Once authentication succeeds, you will log in to the server. The level of commands that you can access after login is authorized by the CAMS server. You can specify the level by setting the **EXEC Privilege Level** argument in the **Add Account** window shown in Figure 1-16.

1.1.2 When Switch Acts as Server for Password and HWTACACS Authentication

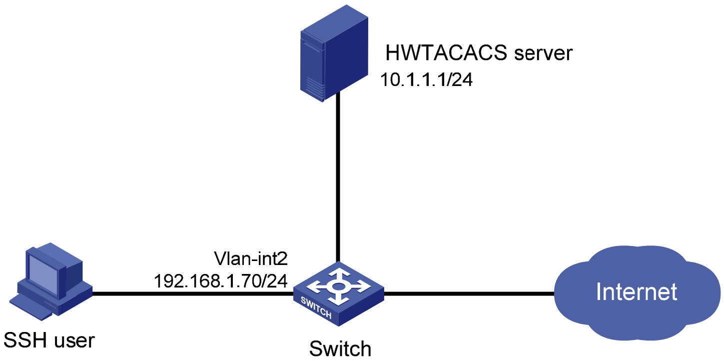
Network requirements

As shown in Figure 1-19, an SSH connection is required between the host (SSH client) and the switch (SSH server) for secure data exchange. Password and HWTACACS authentication is required.

- The host runs SSH2.0 client software to establish a local connection with the switch.
- The switch cooperates with an HWTACACS server to authenticate SSH users.

Network diagram

Figure 1-19 Switch acts as server for password and HWTACACS authentication



Configuration procedure

- Configure the SSH server

Create a VLAN interface on the switch and assign it an IP address. This address will be used as the IP address of the SSH server for SSH connections.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

Caution

Generating the RSA key pair on the server is prerequisite to SSH login.

Generate RSA key pair.

```
[Switch] public-key local create rsa
```

Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
[Switch-ui-vty0-4] quit
```

Configure the HWTACACS scheme.

```
[Switch] hwtacacs scheme hwtac
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49
[Switch-hwtacacs-hwtac] key authentication expert
[Switch-hwtacacs-hwtac] key authorization expert
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
```

Apply the scheme to the ISP domain.

```
[Switch] domain bbb
[Switch-isp-bbb] scheme hwtacacs-scheme hwtac
[Switch-isp-bbb] quit
```

Configure an SSH user, specifying the switch to perform password authentication for the user.

```
[Switch] ssh user client001 authentication-type password
```

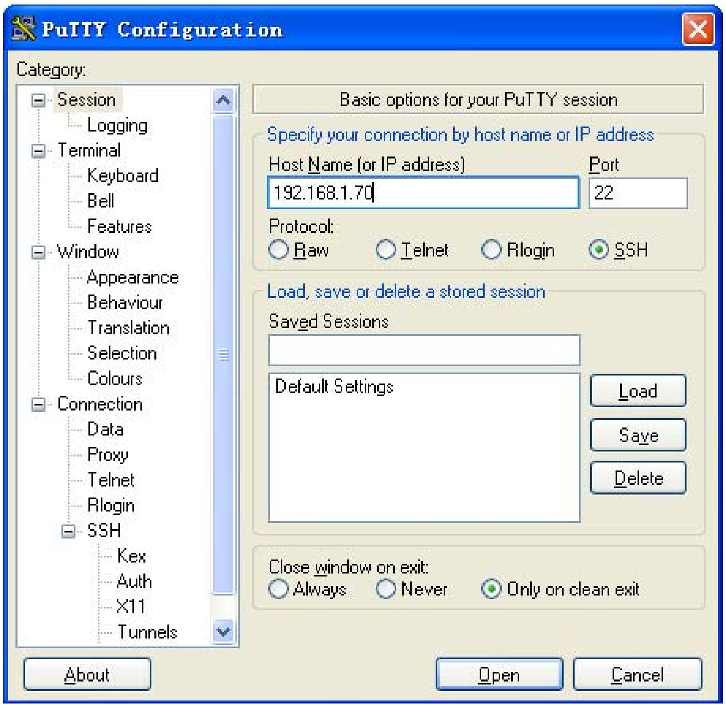
- Configure the SSH client

Configure an IP address (192.168.1.1 in this case) for the SSH client. This IP address and that of the VLAN interface on the switch must be in the same network segment.

Configure the SSH client software to establish a connection to the SSH server. Take SSH client software Putty Version 0.58 as an example:

1) Run PuTTY.exe to enter the following configuration interface.

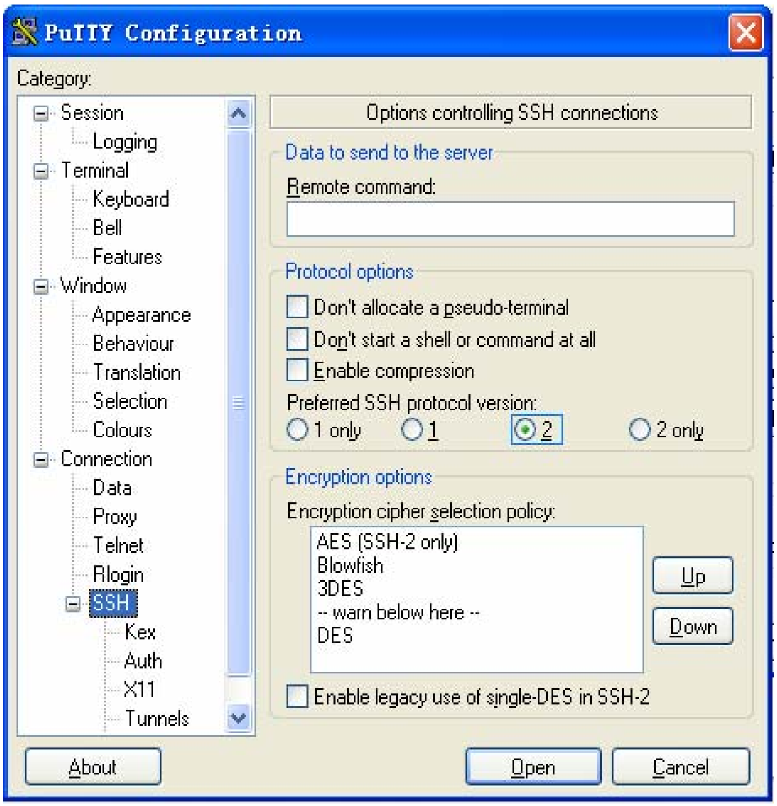
Figure 1-20 SSH client configuration interface (1)



In the **Host Name (or IP address)** text box, enter the IP address of the SSH server.

2) From the category on the left pane of the window, select **Connection** > **SSH**. The window as shown in Figure 1-21 appears.

Figure 1-21 SSH client configuration interface (2)



Under **Protocol options**, select **2** from **Preferred SSH protocol version**. Then, click **Open**. If the connection is normal, you will be prompted to enter the user name **client001** and the password. Once authentication succeeds, you will log in to the server. The level of commands that you can access after login is authorized by the HWTACACS server. For authorization configuration of the HWTACACS server, refer to relevant HWTACACS server configuration manuals.

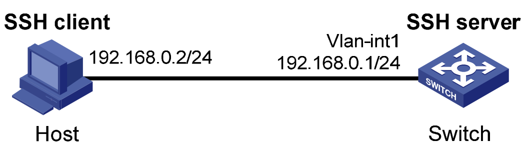
When Switch Acts as Server for Publickey Authentication

Network requirements

As shown in Figure 1-22, establish an SSH connection between the host (SSH client) and the switch (SSH Server) for secure data exchange. The host runs SSH2.0 client software. Publickey authentication is required.

Network diagram

Figure 1-22 Switch acts as server for publickey authentication



Configuration procedure

- Configure the SSH server

Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<Switch> system-view
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[Switch-Vlan-interface1] quit
```

Note

Generating the RSA key pair on the server is prerequisite to SSH login.

Generate RSA key pair.

```
[Switch] public-key local create rsa
```

Set the authentication mode for the user interfaces to AAA.

```
[Switch] user-interface vty 0 4
[Switch-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[Switch-ui-vty0-4] protocol inbound ssh
```

Set the client's command privilege level to 3

```
[Switch-ui-vty0-4] user privilege level 3
[Switch-ui-vty0-4] quit
```

Configure the authentication type of the SSH client named client 001 as publickey.

```
[Switch] ssh user client001 authentication-type publickey
```

Note

Before performing the following steps, you must generate an RSA public key pair (using the client software) on the client, save the key pair in a file named public, and then upload the file to the SSH server through FTP or TFTP. For details, refer to the SSH client configuration part. .

Import the client's public key named **Switch001** from file **public**.

```
[Switch] public-key peer Switch001 import sshkey public
```

Assign the public key **Switch001** to client **client001**.

```
[Switch] ssh user client001 assign publickey Switch001
```

- Configure the SSH client (taking PuTTY version 0.58 as an example)

Generate an RSA key pair.

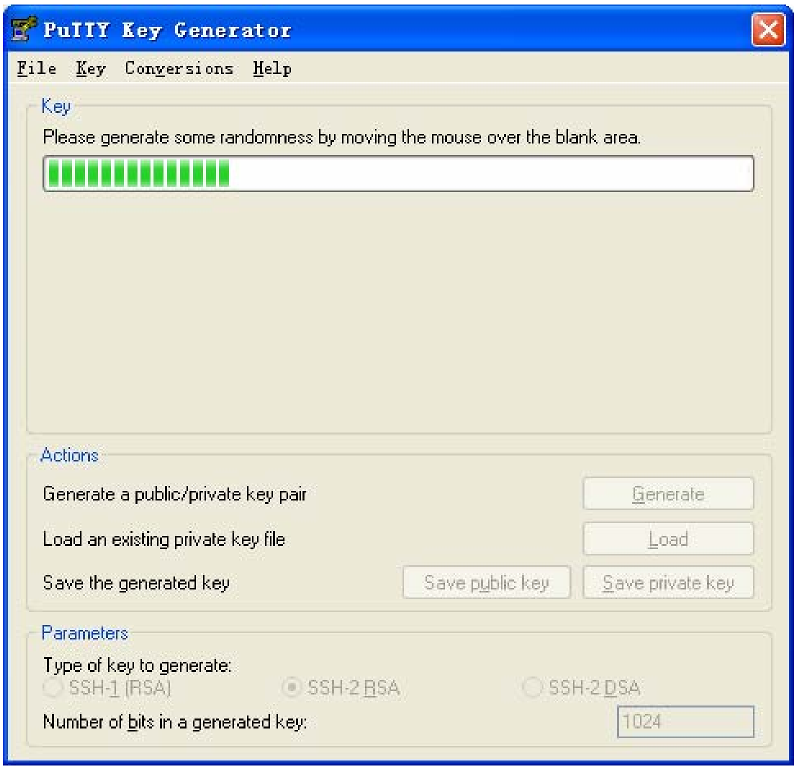
1) Run PuTTYGen.exe, choose **SSH2(RSA)** and click **Generate**.

Figure 1-23 Generate a client key pair (1)

Note

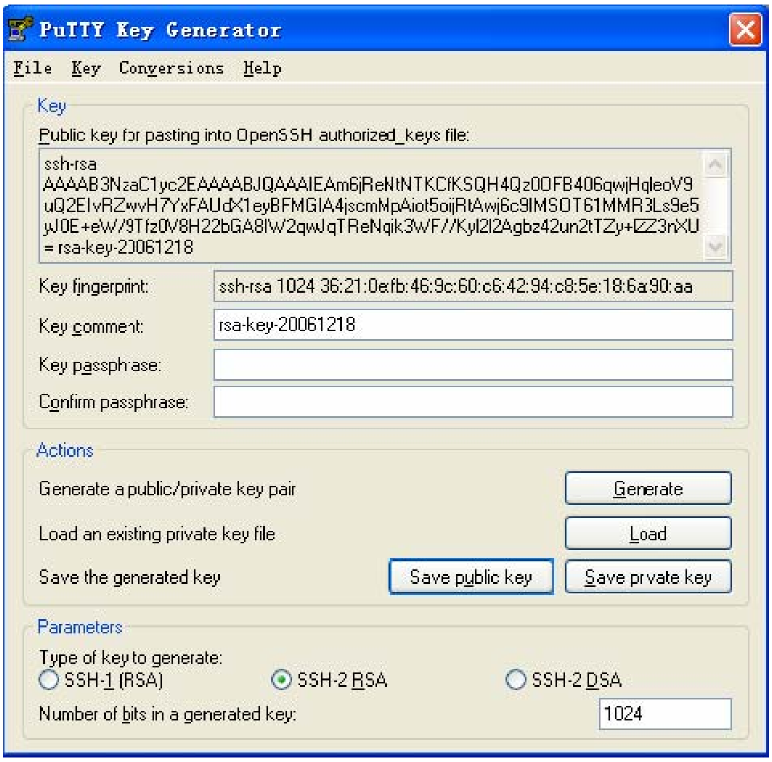
While generating the key pair, you must move the mouse continuously and keep the mouse off the green process bar shown in Figure 1-24. Otherwise, the process bar stops moving and the key pair generating process is stopped.

Figure 1-24 Generate a client key pair (2)



After the key pair is generated, click **Save public key** and enter the name of the file for saving the public key (**public** in this case).

Figure 1-25 Generate a client key pair (3)



Likewise, to save the private key, click **Save private key**. A warning window pops up to prompt you whether to save the private key without any protection. Click **Yes** and enter the name of the file for saving the private key (**private.ppk** in this case).

Figure 1-26 Generate a client key pair (4)

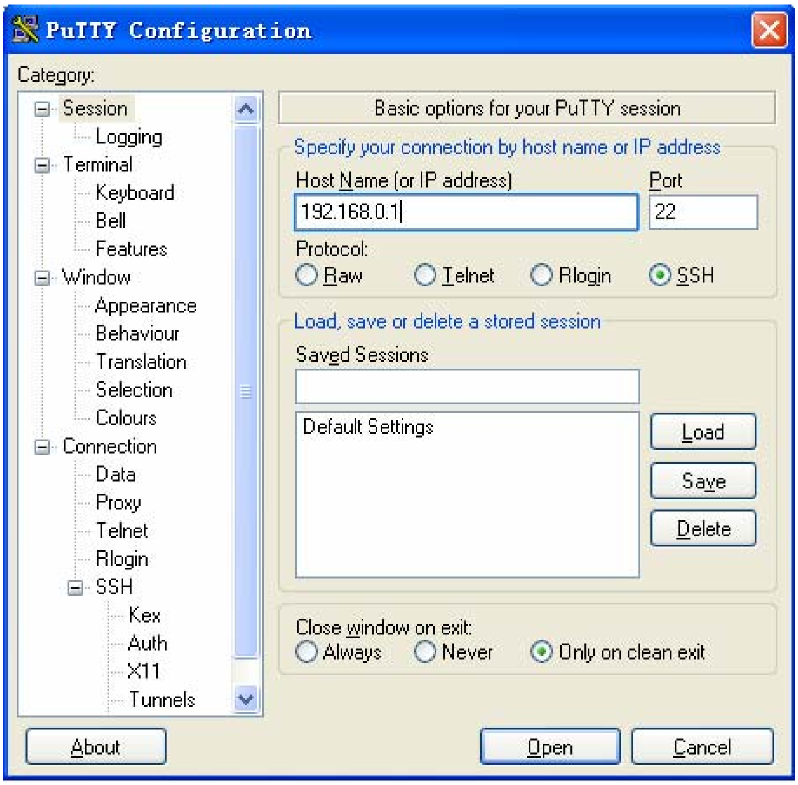
Note

After a public key pair is generated, you need to upload the pubic key file to the server through FTP or TFTP, and complete the server end configuration before you continue to configure the client.

Establish a connection with the SSH server

2) Launch PuTTY.exe to enter the following interface.

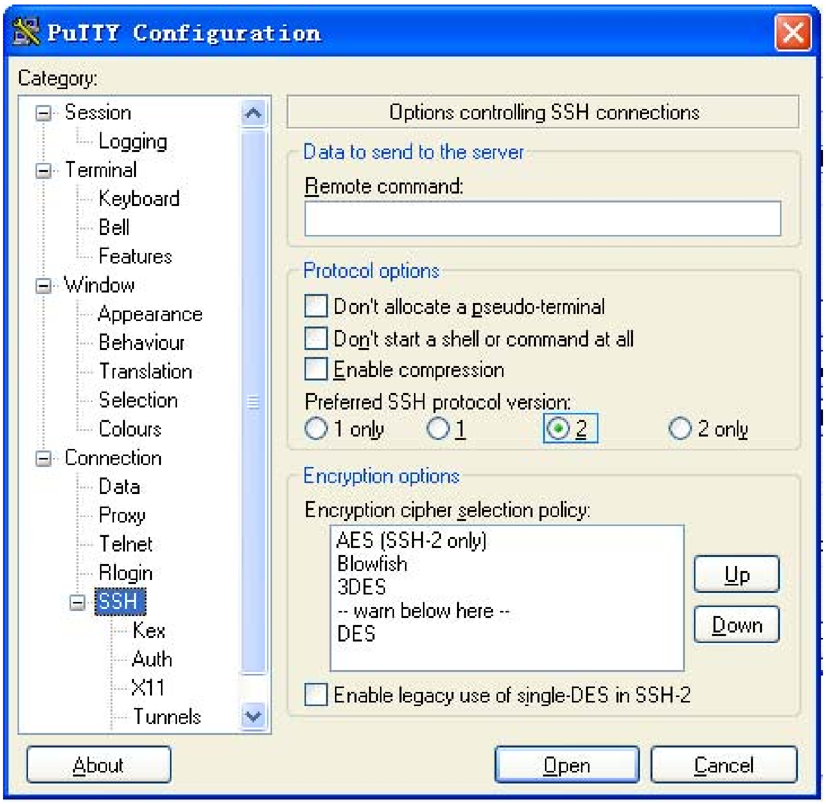
Figure 1-27 SSH client configuration interface (1)



In the **Host Name (or IP address)** text box, enter the IP address of the server.

3) From the category on the left pane of the window, select **SSH** under **Connection**. The window as shown in Figure 1-28 appears.

Figure 1-28 SSH client configuration interface (2)



Under **Protocol options**, select **2** from **Preferred SSH protocol version**.

4) Select **Connection/SSH/Auth**. The following window appears.

Figure 1-29 SSH client configuration interface (3)

Click **Browse** to bring up the file selection window, navigate to the private key file and click **OK**.

5) From the window shown in Figure 1-29, click **Open**. If the connection is normal, you will be prompted to enter the username.

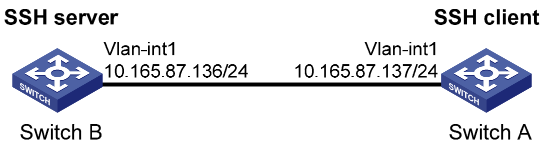
When Switch Acts as Client for Password Authentication

Network requirements

As shown in Figure 1-30, establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name for login is client001 and the SSH server's IP address is 10.165.87.136. Password authentication is required.

Network diagram

Figure 1-30 Switch acts as client for password authentication



Configuration procedure

- Configure Switch B

Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Note

Generating the RSA key pair on the server is prerequisite to SSH login.

Generate RSA key pair.

```
[SwitchB] public-key local create rsa
```

Set the authentication mode for the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
[SwitchB-ui-vty0-4] quit
```

Create local user **client001**, and set the authentication password to **abc**, the login protocol to SSH, and user command privilege level to 3.

```
[SwitchB] local-user client001
```

```
[SwitchB-luser-client001] password simple abc
[SwitchB-luser-client001] service-type ssh level 3
[SwitchB-luser-client001] quit
```

Configure the authentication type of user client001 as password.

```
[SwitchB] ssh user client001 authentication-type password
```

- Configure Switch A

Create a VLAN interface on the switch and assign an IP address, which serves as the SSH client's address in an SSH connection.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Establish a connection to the server 10.165.87.136.

```
[SwitchA] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n
Enter password:

**************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.
*  Without the owner's prior written consent,                              *
*  no decompiling or reverse-engineering shall be allowed.                 *
**************************************************************************

<SwitchB>
```

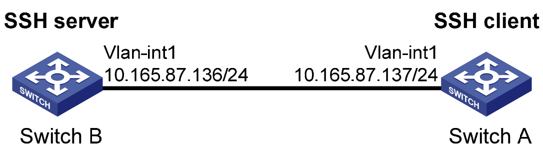
When Switch Acts as Client for Publickey Authentication

Network requirements

As shown in Figure 1-31, establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name is client001 and the SSH server's IP address is 10.165.87.136. Publickey authentication is required.

Network diagram

Figure 1-31 Switch acts as client for publickey authentication



Configuration procedure

- Configure Switch B

Create a VLAN interface on the switch and assign an IP address, which the SSH client will use as the destination for SSH connection.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Note

Generating the RSA key pair on the server is prerequisite to SSH login.

Generate RSA key pair.

```
[SwitchB] public-key local create rsa
```

Set the authentication mode for the user interfaces to AAA.

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

Enable the user interfaces to support SSH.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
```

Set the user command privilege level to 3.

```
[SwitchB-ui-vty0-4] user privilege level 3
[SwitchB-ui-vty0-4] quit
```

Specify the authentication type of user client001 as publickey.

```
[SwitchB] ssh user client001 authentication-type publickey
```

Note

Before doing the following steps, you must first generate a RSA public key pair on the client and save the key pair in a file named Switch001, and then upload the file to the SSH server through FTP or TFTP. For details, refer to “Configure Switch A”.

Import the client public key pair named Switch001 from the file Switch001.

```
[SwitchB] public-key peer Switch001 import sshkey Switch001
```

Assign the public key Switch001 to user client001.

```
[SwitchB] ssh user client001 assign publickey Switch001
```

- Configure Switch A

Create a VLAN interface on the switch and assign an IP address, which serves as the SSH client’s address in an SSH connection.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Generate a RSA key pair

```
[SwitchA] public-key local create rsa
```

Export the generated RSA key pair to a file named Switch001.

```
[SwitchA] public-key local export rsa ssh2 Switch001
```

Note

After the key pair is generated, you need to upload the pubic key file to the server through FTP or TFTP and complete the server end configuration before you continue to configure the client.

Establish an SSH connection to the server 10.165.87.136.

```
[SwitchA] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n

**************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved
*  Without the owner's prior written consent,                                *
*  no decompiling or reverse-engineering shall be allowed.                   *
**************************************************************************

<SwitchB>
```

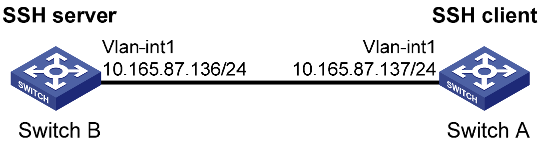
When Switch Acts as Client and First-Time Authentication is not Supported

Network requirements

As shown in Figure 1-32, establish an SSH connection between Switch A (SSH Client) and Switch B (SSH Server) for secure data exchange. The user name is client001 and the SSH server's IP address is 10.165.87.136. The **publickey** authentication mode is used to enhance security.

Network diagram

Figure 1-32 Switch acts as client and first-time authentication is not supported



Configuration procedure

- Configure Switch B

Create a VLAN interface on the switch and assign an IP address for it to serve as the destination of the client.

```
<SwitchB> system-view
[SwitchB] interface vlan-interface 1
[SwitchB-Vlan-interface1] ip address 10.165.87.136 255.255.255.0
[SwitchB-Vlan-interface1] quit
```

Note

Generating the RSA key pair on the server is prerequisite to SSH login.

Generate RSA key pair.

```
[SwitchB] public-key local create rsa
```

Set AAA authentication on user interfaces.

```
[SwitchB] user-interface vty 0 4
[SwitchB-ui-vty0-4] authentication-mode scheme
```

Configure the user interfaces to support SSH.

```
[SwitchB-ui-vty0-4] protocol inbound ssh
```

Set the user command privilege level to 3.

```
[SwitchB-ui-vty0-4] user privilege level 3
[SwitchB-ui-vty0-4] quit
```

Specify the authentication type for user client001 as publickey.

```
[SwitchB] ssh user client001 authentication-type publickey
```

Note

Before doing the following steps, you must first generate a RSA key pair on the client and save the key pair in a file named Switch001, and then upload the file to the SSH server through FTP or TFTP. For details, refer to the following “Configure Switch A”.

Import the client's public key file Switch001 and name the public key as Switch001.

```
[SwitchB] public-key peer Switch001 import sshkey Switch001
```

Assign public key Switch001 to user client001

```
[SwitchB] ssh user client001 assign publickey Switch001
```

Export the generated RSA host public key pair to a file named Switch002.

```
[SwitchB] public-key local export rsa ssh2 Switch002
```

Note

When first-time authentication is not supported, you must first generate a RSA key pair on the server and save the key pair in a file named Switch002, and then upload the file to the SSH client through FTP or TFTP.

- Configure Switch A

Create a VLAN interface on the switch and assign an IP address, which serves as the SSH client's address in an SSH connection.

```
<SwitchA> system-view
[SwitchA] interface vlan-interface 1
[SwitchA-Vlan-interface1] ip address 10.165.87.137 255.255.255.0
[SwitchA-Vlan-interface1] quit
```

Generate a RSA key pair

```
[SwitchA] public-key local create rsa
```

Export the generated RSA key pair to a file named Switch001.

```
[SwitchA] public-key local export rsa ssh2 Switch001
```

Note

After generating the key pair, you need to upload the key pair file to the server through FTP or TFTP and complete the server end configuration before you continue to configure the client.

Disable first-time authentication on the device.

```
[SwitchA] undo ssh client first-time
```

Note

When first-time authentication is not supported, you must first generate a RSA key pair on the server and save the key pair in a file named Switch002, and then upload the file to the SSH client through FTP or TFTP. For details, refer to the above part "Configure Switch B".

Import the public key pair named Switch002 from the file Switch002.

```
[SwitchA] public-key peer Switch002 import sshkey Switch002
```

Specify the host public key pair name of the server.

```
[SwitchA] ssh client 10.165.87.136 assign publickey Switch002
```

Establish the SSH connection to server 10.165.87.136.

```
[SwitchA] ssh2 10.165.87.136
Username: client001
Trying 10.165.87.136 ...
Press CTRL+K to abort
Connected to 10.165.87.136 ...

**************************************************************************
*  Copyright(c) 2004-2008 3Com Corp. and its licensors. All rights reserved.
*  Without the owner's prior written consent,                               *
*  no decompiling or reverse-engineering shall be allowed.                  *
**************************************************************************

<SwitchB>
```

Table of Contents

1 File System Management Configuration

When configuring file system management, go to these sections for information you are interested in:

- File System Configuration
- File Attribute Configuration
- Configuration File Backup and Restoration

File System Configuration

Introduction to File System

To facilitate management on the switch memory, 4500 series Ethernet switches provide the file system function, allowing you to access and manage the files and directories. You can create, remove, copy or delete a file through command lines, and you can manage files using directories.

File System Configuration Task List

Complete the following tasks to configure the file system:

Task	Remarks
Directory Operations	Optional
File Operations	Optional
Flash Memory Operations	Optional
Prompt Mode Configuration	Optional

Note

The 3com 4500 series Ethernet switches support Expandable Resilient Networking (XRN), and allow you to access a file on a switch in one of the following ways:

- To access a file on the specified unit, you need to specify the file in universal resource locator (URL) format and starting with **unit[No.]>flash:/**, where **[No.]** represents the unit ID of the switch. For example, if the unit ID of the switch is 1, the URL of a file named **text.txt** in the root directory of the switch is **unit1>flash:/text.txt**.
- To access a file on the current unit, you need to enter the file URL starting with **flash:/**. For example, the URL of file text.txt in the root directory of the Flash on the current unit is **flash:/text.txt**.
- To access a file in the current directory, enter the path name or file name directly. For example, to access file text.txt in the current directory, you can directly input the file name **text.txt** as the file URL.

Directory Operations

The file system provides directory-related functions, such as:

- Creating/deleting a directory
- Displaying the current work directory, or contents in a specified directory

Follow these steps to perform directory-related operations:

To do…	Use the command…	Remarks
Create a directory	**mkdir** *directory*	Optional Available in user view
Delete a directory	**rmdir** *directory*	Optional Available in user view
Display the current work directory	**pwd**	Optional Available in user view
Display the information about specific directories and files	**dir** [**/all**] [**/fabric** | *file-url*]	Optional Available in user view
Enter a specified directory	**cd** *directory*	Optional Available in user view

Note

- Only empty directories can be deleted by using the **rmdir** command.
- In the output information of the **dir** /**all** command, deleted files (that is, those stored in the recycle bin) are embraced in brackets.

File Operations

Follow these steps to perform file-related operations:

To do…	Use the command…	Remarks
Delete a file	**delete** [**/unreserved**] *file-url* **delete** { **running-files** | **standby-files** } [**/fabric**] [**/unreserved**]	Optional A deleted file can be restored by using the **undelete** command if you delete it by executing the **delete** command without specifying the **/unreserved** keyword. Available in user view
Restore a file in the recycle bin	**undelete** *file-url*	Optional Available in user view
Delete a file from the recycle bin	**reset recycle-bin** [*file-url*] [**/force**] **reset recycle-bin** [**/fabric**]	Optional Available in user view
Upgrade the software of the whole fabric	update fabric *file-name*	Optional Available in user view

To do…	Use the command…	Remarks
Rename a file	**rename** *fileurl-source fileurl-dest*	Optional Available in user view
Copy a file	**copy** *fileurl-source fileurl-dest*	Optional Available in user view
Move a file	**move** *fileurl-source fileurl-dest*	Optional Available in user view
Display the content of a file	**more** *file-url*	Optional Available in user view Currently, the file system only supports displaying the contents of text files.
Display the information about a directory or a file	**dir** [**/all**] [**/fabric** | *file-url*]	Optional Available in user view
Enter system view	**system-view**	—
Execute the specified batch file	**execute** *filename*	Optional Available in system view

Caution

- For deleted files whose names are the same, only the latest deleted file is kept in the recycle bin and can be restored.
- The files which are deleted by the **delete** command without the **/unreserved** keyword are actually moved to the recycle bin and thus still take storage space. You can clear the recycle bin by using the **reset recycle-bin** command.
- Use the **update fabric** command after all traffic flows are stopped.
- The **dir /all** command displays the files in the recycle bin in square brackets.
- If the configuration files are deleted, the switch adopts the null configuration when it starts up next time.

Flash Memory Operations

Follow these steps to perform Flash memory operations:

To do…	Use the command…	Remarks
Format the Flash memory	**format** *device*	Required Available in user view
Restore space on the Flash memory	**fixdisk** *device*	Required Available in user view

Caution

The format operation leads to the loss of all files, including the configuration files, on the Flash memory and is irretrievable.

Prompt Mode Configuration

You can set the prompt mode of the current file system to **alert** or **quiet**. In alert mode, the file system will give a prompt for confirmation if you execute a command which may cause data loss, for example, deleting or overwriting a file. In quiet mode, such prompt will not be displayed.

Follow these steps to set the prompt mode of file system:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the prompt mode of the file system	**file prompt** { **alert** | **quiet** }	Required By default, the prompt mode of the file system is **alert**.

File System Configuration Examples

Display all the files in the root directory of the file system on the local unit.

```
<Sysname> dir /all
Directory of unit1>flash:/

   1 (*)    -rw-    5822215   Jan 01 1970 00:07:03   test.bin
   2        -rwh          4   Apr 01 2000 23:55:49   snmpboots
   3        -rwh        428   Apr 02 2000 00:47:30   hostkey
   4        -rwh        572   Apr 02 2000 00:47:38   serverkey
   5        -rw-       1220   Apr 02 2000 00:06:57   song.cfg
   6        -rw-      26103   Jan 01 1970 00:04:34   testv1r1.bin
   7        -rwh         88   Apr 01 2000 23:55:53   private-data.txt
   8 (*)    -rw-       1376   Apr 02 2000 01:56:28   config.cfg

7239 KB total (2634 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
```

Copy the file **flash:/config.cfg** to **flash:/test/**, with **1.cfg** as the name of the new file.

```
<Sysname> copy flash:/config.cfg flash:/test/1.cfg
Copy unit1>flash:/config.cfg to unit1>flash:/test/1.cfg?[Y/N]:y
..
%Copy file unit1>flash:/config.cfg to unit1>flash:/test/1.cfg...Done.
```

Display the file information after the copy operation.

```
<Sysname> dir /all
```

```
Directory of unit1>flash:/

   1 (*)    -rw-    5822215  Jan 01 1970 00:07:03   test.bin
   2        -rwh          4  Apr 01 2000 23:55:49   snmpboots
   3        -rwh        428  Apr 02 2000 00:47:30   hostkey
   4        -rwh        572  Apr 02 2000 00:47:38   serverkey
   5        -rw-       1220  Apr 02 2000 00:06:57   song.cfg
   6        -rw-      26103  Jan 01 1970 00:04:34   testv1r1.bin
   7        -rwh         88  Apr 01 2000 23:55:53   private-data.txt
   8 (*)    -rw-       1376  Apr 02 2000 01:56:28   config.cfg
   9        drw-          -  Apr 04 2000 04:50:07   test

7239 KB total (2631 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute

<Sysname> dir unit1>flash:/test/
Directory of unit1>flash:/test/

   1        -rw-       1376  Apr 04 2000 04:50:30   1.cfg

7239 KB total (2025 KB free)

(*) -with main attribute   (b) -with backup attribute
(*b) -with both main and backup attribute
```

File Attribute Configuration

Introduction to File Attributes

The following three startup files support file attribute configuration:

- App files: An app file is an executable file, with .bin as the extension.
- Configuration files: A configuration file is used to store and restore configuration, with .cfg as the extension.
- Web files: A Web file is used for Web-based network management, with .web as the extension.

The app files, configuration files, and Web files support three kinds of attributes: main, backup and none, as described in Table 1-1.

Table 1-1 Descriptions on file attributes

Attribute name	Description	Feature	Identifier
main	Identifies main startup files. The main startup file is preferred for a switch to start up.	In the Flash memory, there can be only one app file, one configuration file and one Web file with the main attribute.	(*)

Attribute name	Description	Feature	Identifier
backup	Identifies backup startup files. The backup startup file is used after a switch fails to start up using the main startup file.	In the Flash memory, there can be only one app file, one configuration file and one Web file with the backup attribute.	(b)
none	Identifies files that are neither of main attribute nor backup attribute.	—	None

Note

A file can have both the main and backup attributes. Files of this kind are labeled *b.

Note that, there can be only one app file, one configuration file and one Web file with the main attribute in the Flash memory. If a newly created file is configured to be with the main attribute, the existing file with the main attribute in the Flash memory will lose its main attribute. This circumstance also applies to the file with the backup attribute in the Flash memory.

File operations and file attribute operations are independent. For example, if you delete a file with the main attribute from the Flash memory, the other files in the flash memory will not possess the main attribute. If you download a valid file with the same name as the deleted file to the flash memory, the file will possess the main attribute.

After the Boot ROM of a switch is upgraded, the original default app file has the main attribute.

Booting with the Startup File

The device selects the main startup file as the preferred startup file. If the device fails to boot with the main startup file, it boots with the backup startup file.

For the Web file and configuration file, 3com may provide corresponding default file when releasing software versions. When booting, the device selects the startup files based on certain order. The device selects Web files in the following steps:

1) If the default Web file exists, the device will boot with the default Web file;
2) If the default Web file does not exist, but the main Web file exists, the device will boot with the main Web file;
3) If neither the default Web file nor the main Web file exists, but the backup Web exists, the device will boot with the backup Web file;
4) If neither of the default Web file, main Web file and backup Web exists, the device considers that no Web file exists.

For the selection of the configuration file when the device boots, refer to the *Configuration File Management* part in this manual.

Configuring File Attributes

You can configure and view the main attribute or backup attribute of the file used for the next startup of a switch, and change the main or backup attribute of the file.

Follow these steps to configure file attributes:

To do…	Use the command…	Remarks
Configure the app file with the main attribute for the next startup	**boot boot-loader** *file-url* [**fabric**]	Optional Available in user view
Configure the app file with the backup attribute for the next startup	**boot boot-loader backup-attribute** *file-url* [**fabric**]	Optional Available in user view
Configure the Web file and its attribute	**boot web-package** *webfile* { **backup** | **main** }	Optional Available in user view
Switch the file attributes between main and backup	**boot attribute-switch** { **all** | **app** | **configuration** | **web** } **fabric**	Optional Available in user view
Specify to enable user to use the customized password to enter the BOOT menu	**startup bootrom-access enable**	Optional By default, the user is enabled to use the customized password to enter the BOOT menu. Available in user view
Display the information about the app file used as the startup file	**display boot-loader** [**unit** *unit-id*]	Optional Available in any view
Display information about the Web file used by the device	**display web package**	

Caution

- Before configuring the main or backup attribute for a file in the fabric, make sure the file already exists on all devices in the fabric.
- The configuration of the main or backup attribute of a Web file takes effect immediately without restarting the switch.
- After upgrading a Web file, you need to specify the new Web file in the Boot menu after restarting the switch or specify a new Web file by using the **boot web-package** command. Otherwise, Web server cannot function normally.
- Currently, a configuration file has the extension of cfg and resides in the root directory of the Flash memory.
- For the detailed configuration of configuration file attributes, refer to the *Configuration File Management* module in this manual.

Configuration File Backup and Restoration

Introduction to Configuration File Backup and Restoration

Formerly, you can only back up and restore the configuration file of the units one by one in a fabric system.

By using the configuration file backup and restoration feature, you can easily back up and restore the configuration files in the whole fabric as well as in a specific unit.

In the backup process, the system first saves the current configuration of a unit to the startup configuration file, and then uploads the file to the TFTP server. In the restore process, the system downloads the startup configuration file from the TFTP server to the local unit.

The configurations of different units in the fabric system can be saved in different .cfg configuration files on the TFTP server. These configuration files form the startup configuration of the whole fabric.

File Backup and Restoration

Configuration prerequisites

Before performing the following operations, you must first ensure that:

- The relevant units support TFTP client.
- The TFTP server is started
- A route exists between the TFTP server and TFTP client.

Configuration procedure

Follow these steps to back up and restore configuration file:

To do…	Use the command…	Remarks
Back up the current configuration of a specified unit	**backup unit** *unit-id* **current-configuration to** { *dest-addr* | *dest-hostname* } *filename.cfg*	Optional Available in user view
Back up the current configuration of the whole fabric system	**backup fabric current-configuration to** { *dest-addr* | *dest-hostname* } *filename.cfg*	Optional Available in user view
Restore the startup configuration of a specified unit	**restore unit** *unit-id* **startup-configuration from** { *source-addr* | *source-hostname* } *filename.cfg*	Optional Available in user view
Restore the startup configuration of the whole fabric system	**restore fabric startup-configuration from** { *source-addr* | *source-hostname* } *filename.cfg*	Optional Available in user view

Table of Contents

1 FTP and SFTP Configuration

When configuring FTP and SFTP, go to these sections for information you are interested in:

- Introduction to FTP and SFTP
- FTP Configuration
- SFTP Configuration

Introduction to FTP and SFTP

Introduction to FTP

File Transfer Protocol (FTP) is commonly used in IP-based networks to transmit files. Before World Wide Web comes into being, files are transferred through command lines, and the most popular application is FTP. At present, although E-mail and Web are the usual methods for file transmission, FTP still has its strongholds.

As an application layer protocol, FTP is used for file transfer between remote server and local client. FTP uses TCP ports 20 and 21 for data transfer and control command transfer respectively. Basic FTP operations are described in RFC 959.

FTP-based file transmission is performed in the following two modes:

- Binary mode for program file transfer
- ASCII mode for text file transfer

A 3com switch 4500 can act as an FTP client or the FTP server in FTP-employed data transmission:

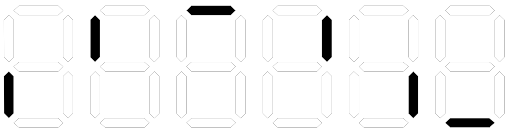
Table 1-1 Roles that a 3com switch 4500 acts as in FTP

Item	Description	Remarks
FTP server	An Ethernet switch can operate as an FTP server to provide file transmission services for FTP clients. You can log in to a switch operating as an FTP server by running an FTP client program on your PC to access files on the FTP server.	The prerequisite is that a route exists between the switch and the PC.
FTP client	In this case, you need to establish a connection between your PC and the switch through a terminal emulation program or Telnet, execute the **ftp** X.X.X.X command on your PC. (X.X.X.X is the IP address of an FTP server or a host name), and enter your user name and password in turn. A switch can operate as an FTP client, through which you can access files on the FTP server.	

- With a 3com switch 4500 serving as an FTP server, the seven-segment digital LED on the front panel of the switch rotates clockwise when an FTP client is uploading files to the FTP server (the 3com switch 4500), and stops rotating when the file uploading is finished, as shown in Figure 1-1.
- With a 3com switch 4500 serving as an FTP client, the seven-segment digital LED on the front panel of the switch rotates clockwise when the FTP client (the 3com switch 4500) is downloading

files from an FTP server, and stops rotating when the file downloading is finished, as shown in Figure 1-1.

Figure 1-1 Clockwise rotating of the seven-segment digital LED



Introduction to SFTP

Secure FTP (SFTP) is established based on an SSH2 connection. It allows a remote user to log in to a switch to manage and transmit files, providing a securer guarantee for data transmission. In addition, since the switch can be used as a client, you can log in to remote devices to transfer files securely.

FTP Configuration

Complete the following tasks to configure FTP:

Task		Remarks
FTP Configuration: A Switch Operating as an FTP Server	Creating an FTP user	Required
	Enabling an FTP server	Required
	Configuring connection idle time	Optional
	Specifying the source interface and source IP address for an FTP server	Optional
	Disconnecting a specified user	Optional
	Configuring the banner for an FTP server	Optional
	Displaying FTP server information	Optional
FTP Configuration: A Switch Operating as an FTP Client	Basic configurations on an FTP client	—
	Specifying the source interface and source IP address for an FTP client	Optional

FTP Configuration: A Switch Operating as an FTP Server

Creating an FTP user

Configure the user name and password for the FTP user and set the service type to FTP. To use FTP services, a user must provide a user name and password for being authenticated by the FTP server. Only users that pass the authentication have access to the FTP server.

Follow these steps to create an FTP user:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Add a local user and enter local user view	**local-user** *user-name*	Required By default, no local user is configured.

To do…	Use the command…	Remarks
Configure a password for the specified user	**password** { **simple** | **cipher** } *password*	Optional By default, no password is configured.
Configure the service type as FTP	**service-type ftp**	Required By default, no service is configured.

Enabling an FTP server

Follow these steps to enable an FTP server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the FTP server function	**ftp server enable**	Required Disabled by default.

Note

- Only one user can access a 3com switch 4500 at a given time when the latter operates as an FTP server.
- Operating as an FTP server, a 3com switch 4500 cannot receive a file whose size exceeds its storage space. The clients that attempt to upload such a file will be disconnected with the FTP server due to lack of storage space on the FTP server.
- When you log in to a Fabric consisting of multiple switches through an FTP client, after the FTP client passes authentication, you can log in to the master device of the Fabric.
- You cannot access a 3com switch 4500 operating as an FTP server through Microsoft Internet Explorer. To do so, use other client software.

Note

To protect unused sockets against attacks, the 3com switch 4500 provides the following functions:

- TCP 21 is enabled only when you start the FTP server.
- TCP 21 is disabled when you shut down the FTP server.

Configuring connection idle time

After the idle time is configured, if the server does not receive service requests from a client within a specified time period, it terminates the connection with the client, thus preventing a user from occupying the connection for a long time without performing any operation.

Follow these steps to configure connection idle time:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the connection idle time for the FTP server	**ftp timeout** *minutes*	Optional 30 minutes by default

Specifying the source interface and source IP address for an FTP server

You can specify the source interface and source IP address for an FTP server to enhance server security. After this configuration, FTP clients can access this server only through the IP address of the specified interface or the specified IP address.

Note

Source interface refers to the existing VLAN interface or Loopback interface on the device. Source IP address refers to the IP address configured for the interface on the device. Each source interface corresponds to a source IP address. Therefore, specifying a source interface for the FTP server is the same as specifying the IP address of this interface as the source IP address.

Follow these steps to specify the source interface and source IP address for an FTP server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify the source interface for an FTP server	**ftp-server source-interface** *interface-type interface-number*	Use either command Not specified by default.
Specifying the source IP address for an FTP server	**ftp-server source-ip** *ip-address*	

Note

- The specified interface must be an existing one. Otherwise a prompt appears to show that the configuration fails.
- The value of the *ip-address* argument must be an IP address on the device where the configuration is performed. Otherwise a prompt appears to show that the configuration fails.
- You can specify only one source interface or source IP address for the FTP at one time. That is, only one of the commands **ftp-server source-interface** and **ftp-server source-ip** can be valid at one time. If you execute both of them, the new setting will overwrite the original one.
- If the switch (FTP server) is the command switch or member switch in a cluster, do not use the **ftp-server source-ip** command to specify the private IP address of the cluster as the source IP address of the FTP server. Otherwise, FTP does not take effect.

Disconnecting a specified user

On the FTP server, you can disconnect a specified user from the FTP server to secure the network.

Follow these steps to disconnect a specified user:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
On the FTP server, disconnect a specified user from the FTP server	**ftp disconnect** *user-name*	Required

Note

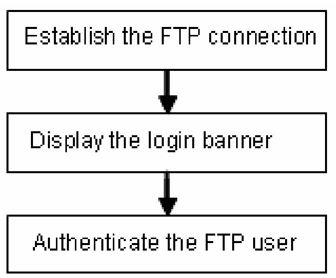
With a 3com switch 4500 acting as the FTP server, if a network administrator attempts to disconnect a user that is uploading/downloading data to/from the FTP server the 3com switch 4500 will disconnect the user after the data transmission is completed.

Configuring the banner for an FTP server

Displaying a banner: With a banner configured on the FTP server, when you access the FTP server through FTP, the configured banner is displayed on the FTP client. Banner falls into the following two types:

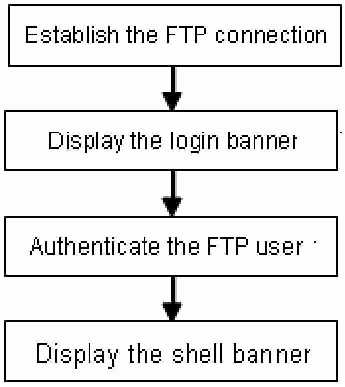
- Login banner: After the connection between an FTP client and an FTP server is established, the FTP server outputs the configured login banner to the FTP client terminal.

Figure 1-2 Process of displaying a login banner



- Shell banner: After the connection between an FTP client and an FTP server is established and correct user name and password are provided, the FTP server outputs the configured shell banner to the FTP client terminal.

Figure 1-3 Process of displaying a shell banner



Follow these steps to configure the banner display for an FTP server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a login banner	**header login** *text*	Required Use either command or both. By default, no banner is configured.
Configure a shell banner	**header shell** *text*	

Note

For details about the **header** command, refer to the Login part of the manual.

Displaying FTP server information

To do…	Use the command…	Remarks
Display the information about FTP server configurations on a switch	**display ftp-server**	Available in any view
Display the source IP address set for an FTP server	**display ftp-server source-ip**	
Display the login FTP client on an FTP server	**display ftp-user**	

FTP Configuration: A Switch Operating as an FTP Client

Basic configurations on an FTP client

By default a switch can operate as an FTP client. In this case, you can connect the switch to the FTP server to perform FTP-related operations (such as creating/removing a directory) by executing commands on the switch.

Follow these steps to perform basic configurations on an FTP client:

To do…	Use the command…	Remarks
Enter FTP client view	**ftp** [**cluster** | *remote-server* [*port-number*]]	—
Specify to transfer files in ASCII characters	**ascii**	Use either command. By default, files are transferred in ASCII characters.
Specify to transfer files in binary streams	**binary**	
Set the data transfer mode to passive	**passive**	Optional **passive** by default.
Change the working directory on the remote FTP server	**cd** *pathname*	Optional
Change the working directory to be the parent directory	**cdup**	
Get the local working path on the FTP client	**lcd**	
Display the working directory on the FTP server	**pwd**	
Create a directory on the remote FTP server	**mkdir** *pathname*	
Remove a directory on the remote FTP server	**rmdir** *pathname*	
Delete a specified file	**delete** *remotefile*	
Query a specified file on the FTP server	**dir** [*remotefile*] [*localfile*]	Optional If no file name is specified, all the files in the current directory are displayed. The difference between these two commands is that the **dir** command can display the file name, directory as well as file attributes; while the **ls** command can display only the file name and directory.
	ls [*remotefile*] [*localfile*]	

To do…	Use the command…	Remarks
Download a remote file from the FTP server	**get** *remotefile* [*localfile*]	Optional
Upload a local file to the remote FTP server	**put** *localfile* [*remotefile*]	
Rename a file on the remote server	**rename** *remote-source remote-dest*	
Log in with the specified user name and password	**user** *username* [*password*]	
Connect to a remote FTP server	**open** { *ip-address* | *server-name* } [*port*]	
Terminate the current FTP connection without exiting FTP client view	**disconnect**	
	close	
Terminate the current FTP connection and return to user view	**quit**	
	bye	
Display the online help about a specified command concerning FTP	**remotehelp** [*protocol-command*]	
Enable the verbose function	**verbose**	Optional Enabled by default.

Specifying the source interface and source IP address for an FTP client

You can specify the source interface and source IP address for a switch acting as an FTP client, so that it can connect to a remote FTP server.

Follow these steps to specify the source interface and source IP address for an FTP client:

To do…	Use the command…	Remarks
Specify the source interface used for the current connection	**ftp** { **cluster** | *remote-server* } **source-interface** *interface-type interface-number*	Optional
Specify the source IP address used for the current connection	**ftp** { **cluster** | *remote-server* } **source-ip** *ip-address*	Optional
Enter system view	**system-view**	—
Specify an interface as the source interface the FTP client uses every time it connects to an FTP server	**ftp source-interface** *interface-type interface-number*	Use either command Not specified by default
Specify an IP address as the source IP address the FTP client uses every time it connects to an FTP server	**ftp source-ip** *ip-address*	
Display the source IP address used by an FTP client every time it connects to an FTP server	**display ftp source-ip**	Available in any view

![Note]

Note

- The specified interface must be an existing one. Otherwise a prompt appears to show that the configuration fails.
- The value of the *ip-address* argument must be the IP address of the device where the configuration is performed. Otherwise a prompt appears to show that the configuration fails.
- The source interface/source IP address set for one connection is prior to the fixed source interface/source IP address set for each connection. That is, for a connection between an FTP client and an FTP server, if you specify the source interface/source IP address used for the connection this time, and the specified source interface/source IP address is different from the fixed one, the former will be used for the connection this time.
- Only one fixed source interface or source IP address can be set for the FTP client at one time. That is, only one of the commands **ftp source-interface** and **ftp source-ip** can be valid at one time. If you execute both of them, the new setting will overwrite the original one.

Configuration Example: A Switch Operating as an FTP Server

Network requirements

A switch operates as an FTP server and a remote PC as an FTP client. The application **switch.bin** of the switch is stored on the PC. Upload the application to the remote switch through FTP and use the **boot boot-loader** command to specify **switch.bin** as the application for next startup. Reboot the switch to upgrade the switch application and download the configuration file **config.cfg** from the switch, thus to back up the configuration file.

- Create a user account on the FTP server with the username **switch** and password **hello**.
- The IP addresses 1.1.1.1 for a VLAN interface on the switch and 2.2.2.2 for the PC have been configured. Ensure that a route exists between the switch and the PC.

Network diagram

Figure 1-4 Network diagram for FTP configurations: a switch operating as an FTP server

Configuration procedure

1) Configure Switch A (the FTP server)

Log in to the switch and enable the FTP server function on the switch. Configure the user name and password used to access FTP services, and specify the service type as FTP (You can log in to a switch through the Console port or by telnetting the switch. See the *Login* module for detailed information.)

Configure the FTP username as **switch**, the password as **hello**, and the service type as FTP.

```
<Sysname>
<Sysname> system-view
[Sysname] ftp server enable
```

```
[Sysname] local-user switch
[Sysname-luser-switch] password simple hello
[Sysname-luser-switch] service-type ftp
```

2) Configure the PC (FTP client)

Run an FTP client application on the PC to connect to the FTP server. Upload the application named **switch.bin** to the root directory of the Flash memory of the FTP server, and download the configuration file named **config.cfg** from the FTP server. The following takes the command line window tool provided by Windows as an example:

Enter the command line window and switch to the directory where the file **switch.bin** is located. In this example it is in the root directory of C:\.

```
C:\>
```

Access the Ethernet switch through FTP. Input the username **switch** and password **hello** to log in and enter FTP view.

```
C:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220 FTP service ready.
User (1.1.1.1:(none)): switch
331 Password required for switch.
Password:
230 User logged in.
ftp>
```

Upload file **switch.bin**.

```
ftp> put switch.bin
200 Port command okay.
150 Opening ASCII mode data connection for switch.bin.
226 Transfer complete.
ftp: 75980 bytes received in 5.55 seconds 13.70Kbytes/sec.
```

Download file **config.cfg**.

```
ftp> get config.cfg
200 Port command okay.
150 Opening ASCII mode data connection for config.cfg.
226 Transfer complete.
ftp: 3980 bytes received in 8.277 seconds 0.48Kbytes/sec.
```

This example uses the command line window tool provided by Windows. When you log in to the FTP server through another FTP client, refer to the corresponding instructions for operation description.

Caution

- If available space on the Flash memory of the switch is not enough to hold the file to be uploaded, you need to delete files not in use from the Flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted. If you have to delete the files in use to make room for the file to be uploaded, you can only delete/download them through the Boot ROM menu.
- 3com switch is not shipped with FTP client application software. You need to purchase and install it by yourself.

3) Configure Switch A (FTP server)

After uploading the application, use the **boot boot-loader** command to specify the uploaded file (**switch.bin**) to be the startup file used when the switch starts the next time, and restart the switch. Thus the switch application is upgraded.

```
<Sysname> boot boot-loader switch.bin
<Sysname> reboot
```

Note

For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to the System Maintenance and Debugging part of this manual.

FTP Banner Display Configuration Example

Network requirements

Configure the Ethernet switch as an FTP server and the remote PC as an FTP client. After a connection between the FTP client and the FTP server is established and login succeeds, the banner is displayed on the FTP client.

- An FTP user with username **switch** and the password **hello** has been configured on the FTP server.
- The IP addresses 1.1.1.1 for a VLAN interface on the switch and 2.2.2.2 for the PC have been configured. Ensure that a route exists between the switch and the PC.
- Configure the login banner of the switch as “login banner appears” and the shell banner as “shell banner appears”.

Network diagram

Figure 1-5 Network diagram for FTP banner display configuration

Configuration procedure

1) Configure the switch (FTP server)

Configure the login banner of the switch as "login banner appears" and the shell banner as "shell banner appears". For detailed configuration of other network requirements, see section Configuration Example: A Switch Operating as an FTP Server.

```
<Sysname> system-view
[Sysname] header login %login banner appears%
[Sysname] header shell %shell banner appears%
```

2) Configure the PC (FTP client)

Access the Ethernet switch through FTP. Enter the username **switch** and the password **hello** to log in to the switch, and then enter FTP view. Login banner appears after FTP connection is established. Shell banner appears after the user passes the authentication.

```
C:\> ftp 1.1.1.1
Connected to 1.1.1.1.
220-login banner appears
220 FTP service ready.
User (1.1.1.1:(none)): switch
331 Password required for switch.
Password:
230-shell banner appears
230 User logged in.
ftp>
```

FTP Configuration: A Switch Operating as an FTP Client

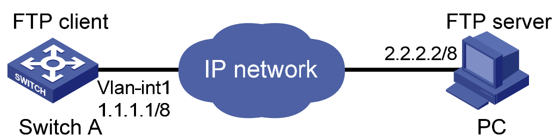
Network requirements

A switch operates as an FTP client and a remote PC as an FTP server. The switch application named **switch.bin** is stored on the PC. Download it to the switch through FTP and use the **boot boot-loader** command to specify **switch.bin** as the application for next startup. Reboot the switch to upgrade the switch application, and then upload the switch configuration file named **config.cfg** to directory **switch** of the PC to back up the configuration file.

- Create a user account on the FTP server with the username **switch** and password **hello**, and grant the user **switch** read and write permissions for the directory **switch** on the PC.
- Configure the IP address 1.1.1.1 for a VLAN interface on the switch, and 2.2.2.2 for the PC. Ensure a route exists between the switch and the PC.

Network diagram

Figure 1-6 Network diagram for FTP configurations: a switch operating as an FTP client



Configuration procedure

1) Configure the PC (FTP server)

Perform FTP server–related configurations on the PC, that is, create a user account on the FTP server with username **switch** and password **hello**. (For detailed configuration, refer to the configuration instruction relevant to the FTP server software.)

2) Configure the switch (FTP client)

Log in to the switch. (You can log in to a switch through the Console port or by telnetting the switch. See the *Login* module for detailed information.)

```
<Sysname>
```

Caution

If available space on the Flash memory of the switch is not enough to hold the file to be uploaded, you need to delete files not in use from the Flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted. If you have to delete the files in use to make room for the file to be uploaded, you can only delete/download them through the Boot ROM menu.

Connect to the FTP server using the **ftp** command in user view. You need to provide the IP address of the FTP server, the user name and the password as well to enter FTP view.

```
<Sysname> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 FTP service ready.
User(none):admin
331 Password required for admin.
Password:
230 User logged in.
[ftp]
```

Enter the authorized directory on the FTP server.

```
[ftp] cd switch
```

Execute the **put** command to upload the configuration file named **config.cfg** to the FTP server.

```
[ftp] put config.cfg
```

Execute the **get** command to download the file named **switch.bin** to the Flash memory of the switch.

```
[ftp] get switch.bin
```

Execute the **quit** command to terminate the FTP connection and return to user view.

```
[ftp] quit
<Sysname>
```

After downloading the file, use the **boot boot-loader** command to specify the downloaded file (**switch.bin**) to be the application for next startup, and then restart the switch. Thus the switch application is upgraded.

```
<Sysname> boot boot-loader switch.bin
<Sysname> reboot
```

Note

For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to the *System Maintenance and Debugging* module of this manual.

SFTP Configuration

Complete the following tasks to configure SFTP:

Task		Remarks
SFTP Configuration: A Switch Operating as an SFTP Server	Enabling an SFTP server	Required
	Configuring connection idle time	Optional
	Supported SFTP client software	—
SFTP Configuration: A Switch Operating as an SFTP Client	Basic configurations on an SFTP client	—
	Specifying the source interface or source IP address for an SFTP client	Optional

SFTP Configuration: A Switch Operating as an SFTP Server

Enabling an SFTP server

Before enabling an SFTP server, you need to enable the SSH server function and specify the service type of the SSH user as **SFTP** or **all**. For details, see the SSH server configuration part of *SSH Operation Manual* of this manual.

Follow these steps to enable an SFTP server:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable an SFTP server	**sftp server enable**	Required Disabled by default.

Configuring connection idle time

After the idle time is configured, if the server does not receive service requests from a client within a specified time period, it terminates the connection with the client, thus preventing a user from occupying the connection for a long time without performing any operation.

Follow these steps to configure connection idle time:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the connection idle time for the SFTP server	**ftp timeout** *time-out-value*	Optional 10 minutes by default.

Supported SFTP client software

A 3com switch 4500 operating as an SFTP server can interoperate with SFTP client software, including SSH Tectia Client v4.2.0 (SFTP), v5.0, and WINSCP.

SFTP client software supports the following operations: logging in to a device; uploading a file; downloading a file; creating a directory; modify a file name or a directory name; browsing directory structure; and manually terminating a connection.

For configurations on client software, see the corresponding configuration manual.

Note

- Currently a 3com switch 4500 operating as an SFTP server supports the connection of only one SFTP user. When multiple users attempt to log in to the SFTP server or multiple connections are enabled on a client, only the first user can log in to the SFTP user. The subsequent connection will fail.
- When you upload a large file through WINSCP, if a file with the same name exists on the server, you are recommended to set the packet timeout time to over 600 seconds, thus to prevent the client from failing to respond to device packets due to timeout. Similarly, when you delete a large file from the server, you are recommended to set the client packet timeout time to over 600 seconds.

SFTP Configuration: A Switch Operating as an SFTP Client

Basic configurations on an SFTP client

By default a switch can operate as an SFTP client. In this case you can connect the switch to the SFTP server to perform SFTP-related operations (such as creating/removing a directory) by executing commands on the switch.

Follow these steps to perform basic configurations on an SFTP client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—

To do…	Use the command…	Remarks
Enter SFTP client view	**sftp** { *host-ip* | *host-name* } [*port-num*] [**identity-key** { **dsa** | **rsa** } | **prefer_kex** { **dh_group1** | **dh_exchange_group** } | **prefer_ctos_cipher** { **3des** | **des | aes128** } | **prefer_stoc_cipher** { **3des** | **des | aes128** } | **prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** } | **prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] *	Required Support for the 3des keyword depends on the number of encryption bits of the software version. The 168-bit version supports this keyword, while the 56-bit version does not.
Change the working directory on the remote SFTP server	**cd** *pathname*	Optional
Change the working directory to be the parent directory	**cdup**	Optional
Display the working directory on the SFTP server	**pwd**	Optional
Create a directory on the remote SFTP server	**mkdir** *pathname*	Optional
Remove a directory on the remote SFTP server	**rmdir** *pathname*	Optional
Delete a specified file	**delete** *remotefile*	Optional Both commands have the same effect.
Delete a specified file	**remove** *remote-file*	Optional Both commands have the same effect.
Query a specified file on the SFTP server	**dir** [**-a** | **-l**] [*remote-path*]	Optional If no file name is provided, all the files in the current directory are displayed. The difference between these two commands is that the **dir** command can display the file name, directory as well as file attributes; while the **ls** command can display only the file name and directory.
Query a specified file on the SFTP server	**ls** [**-a** | **-l**] [*remote-path*]	Optional If no file name is provided, all the files in the current directory are displayed. The difference between these two commands is that the **dir** command can display the file name, directory as well as file attributes; while the **ls** command can display only the file name and directory.
Download a remote file from the SFTP server	**get** *remotefile* [*localfile*]	Optional
Upload a local file to the remote SFTP server	**put** *localfile* [*remotefile*]	Optional
Rename a file on the remote server	**rename** *remote-source remote-dest*	Optional
Exit SFTP client view and return to system view	**bye**	The three commands have the same effect.
Exit SFTP client view and return to system view	**exit**	The three commands have the same effect.
Exit SFTP client view and return to system view	**quit**	The three commands have the same effect.
Display the online help about a specified command concerning SFTP	**help** [**all** | *command-name*]	Optional

Note

If you specify to authenticate a client through public key on the server, the client needs to read the local private key when logging in to the SFTP server. Since both RSA and DSA are available for public key authentication, you need to use the **identity-key** key word to specify the algorithms to get correct local private key; otherwise you will fail to log in. For details, see *SSH Operation Manual*.

Specifying the source interface or source IP address for an SFTP client

You can specify the source interface or source IP address for a switch acting as an FTP client, so that it can connect to a remote SFTP server.

Follow these steps to specify the source interface or source IP address for an SFTP client:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Specify an interface as the source interface of the specified SFTP client	**sftp source-interface** *interface-type interface-number*	Use either command Not specified by default.
Specify an IP address as the source IP address of the specified SFTP client	**sftp source-ip** *ip-address*	
Display the source IP address used by the current SFTP client	**display sftp source-ip**	Optional Available in any view

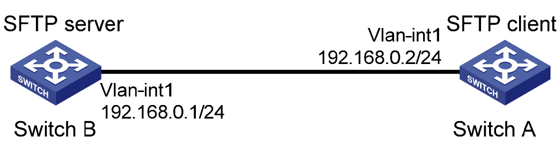
SFTP Configuration Example

Network requirements

As shown in Figure 1-7, establish an SSH connection between the SFTP client (switch A) and the SFTP server (switch B). Log in to switch B through switch A to manage and transmit files. An SFTP user with the username **client001** and password **abc** exists on the SFTP server.

Network diagram

Figure 1-7 Network diagram for SFTP configuration



Configuration procedure

1) Configure the SFTP server (switch B)

Create key pairs.

```
<Sysname> system-view
[Sysname] public-key local create rsa
```

```
[Sysname] public-key local create dsa
```

Create a VLAN interface on the switch and assign to it an IP address, which is used as the destination address for the client to connect to the SFTP server.

```
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 192.168.0.1 255.255.255.0
[Sysname-Vlan-interface1] quit
```

Specify the SSH authentication mode as **AAA**.

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme
```

Configure the protocol through which the remote user logs in to the switch as SSH.

```
[Sysname-ui-vty0-4] protocol inbound ssh
[Sysname-ui-vty0-4] quit
```

Create a local user client001.

```
[Sysname] local-user client001
[Sysname-luser-client001] password simple abc
[Sysname-luser-client001] service-type ssh
[Sysname-luser-client001] quit
```

Configure the authentication mode as **password**. Authentication timeout time, retry number, and update time of the server key adopt the default values.

```
[Sysname] ssh user client001 authentication-type password
```

Specify the service type as SFTP.

```
[Sysname] ssh user client001 service-type sftp
```

Enable the SFTP server.

```
[Sysname] sftp server enable
```

2) Configure the SFTP client (switch A)

Configure the IP address of the VLAN interface on switch A. It must be in the same segment with the IP address of the VLAN interface on switch B. In this example, configure it as 192.168.0.2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 192.168.0.2 255.255.255.0
[Sysname-Vlan-interface1] quit
```

Connect to the remote SFTP server. Enter the username **client001** and the password **abc**, and then enter SFTP client view.

```
[Sysname] sftp 192.168.0.1
Input Username: client001
Trying 192.168.0.1 ...
Press CTRL+K to abort
Connected to 192.168.0.1 ...

The Server is not authenticated. Do you continue to access it?(Y/N):y
Do you want to save the server's public key?(Y/N):n
Enter password:
```

```
sftp-client>
```

Display the current directory of the server. Delete the file **z** and verify the result.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
Received status: End of file
Received status: Success
sftp-client> delete z
The following files will be deleted:
/z
Are you sure to delete it?(Y/N):y
This operation may take a long time.Please wait...

Received status: Success
File successfully Removed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
Received status: End of file
Received status: Success
```

Add a directory **new1**, and then check whether the new directory is successfully created.

```
sftp-client> mkdir new1
Received status: Success
New directory created
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
Received status: End of file
Received status: Success
```

Rename the directory **new1** as **new2**, and then verify the result.

```
sftp-client> rename new1 new2
File successfully renamed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
```

```
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
Received status: End of file
Received status: Success
```

Download the file **pubkey2** from the server and rename it as **public**.

```
sftp-client> get pubkey2 public
This operation may take a long time, please wait...
.
Remote  file:/pubkey2 --->  Local file: public..
Received status: End of file
Received status: Success
Downloading file successfully ended
```

Upload file **pu** to the server and rename it as **puk**, and then verify the result.

```
sftp-client> put pu puk
This operation may take a long time, please wait...
Local file: pu --->  Remote file: /puk
Received status: Success
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pub
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
Received status: End of file
Received status: Success
sftp-client>
```

Exit SFTP.

```
sftp-client> quit
Bye
[Sysname]
```

2 TFTP Configuration

When configuring TFTP, go to these sections for information you are interested in:

- Introduction to TFTP
- TFTP Configuration

Introduction to TFTP

Compared with FTP, Trivial File Transfer Protocol (TFTP) features simple interactive access interface and no authentication control. Therefore, TFTP is applicable in the networks where client-server interactions are relatively simple. TFTP is implemented based on UDP. It transfers data through UDP port 69. Basic TFTP operations are described in RFC 1986.

TFTP transmission is initiated by clients, as described in the following:

- To download a file, a client sends Read Request packets to the TFTP server, then receives data from the TFTP server, and sends acknowledgement packets to the TFTP server.
- To upload a file, a client sends Write Request packets to the TFTP server, then sends data to the TFTP server, and receives acknowledgement packets from the TFTP server.

A 3com switch 4500 can act as a TFTP client only.

When a 3com switch 4500 serving as a TFTP client downloads files from the TFTP server, the seven-segment digital LED on the front panel of the switch rotates clockwise, and it stops rotating when the file downloading is finished, as shown in Figure 1-1.

When you download a file that is larger than the free space of the switch's flash memory:

- If the TFTP server supports file size negotiation, file size negotiation will be initiated between the switch and the server and the file download operation will be aborted if the free space of the switch's flash memory is found to be insufficient.
- If the TFTP server does not support file size negotiation, the switch will receive data from the server until the flash memory is full. If there is more data to be downloaded, the switch will prompt that the space is insufficient and delete the data partially downloaded. File download fails.

TFTP-based file transmission can be performed in the following modes:

- Binary mode for program file transfer.
- ASCII mode for text file transfer.

Note

Before performing TFTP-related configurations, you need to configure IP addresses for the TFTP client and the TFTP server, and make sure a route exists between the two.

TFTP Configuration

Complete the following tasks to configure TFTP:

Task		Remarks
TFTP Configuration: A Switch Operating as a TFTP Client	Basic configurations on a TFTP client	—
	Specifying the source interface or source IP address for an FTP client	Optional
TFTP server configuration	For details, see the corresponding manual	—

TFTP Configuration: A Switch Operating as a TFTP Client

Basic configurations on a TFTP client

By default a switch can operate as a TFTP client. In this case you can connect the switch to the TFTP server to perform TFTP-related operations (such as creating/removing a directory) by executing commands on the switch.

Follow these steps to perform basic configurations on a TFTP client:

To do…	Use the command…	Remarks
Download a file from a TFTP server	**tftp** *tftp-server* **get** *source-file* [*dest-file*]	Optional
Upload a file to a TFTP server	**tftp** *tftp-server* **put** *source-file* [*dest-file*]	Optional
Enter system view	**system-view**	—
Set the file transmission mode	**tftp** { **ascii** | **binary** }	Optional Binary by default.
Specify an ACL rule used by the specified TFTP client to access a TFTP server	**tftp-server acl** acl-number	Optional Not specified by default.

Specifying the source interface or source IP address for an FTP client

You can specify the source interface and source IP address for a switch operating as a TFTP client, so that it can connect with a remote TFTP server through the IP address of the specified interface or the specified IP address.

Follow these steps to specify the source interface and source IP address for a TFTP client:

To do…	Use the command…	Remarks
Specify the source interface used for the current connection	**tftp** *tftp-server* **source-interface** *interface-type interface-number* { **get** *source-file* [*dest-file*] | **put** *source-file-url* [*dest-file*] }	Optional Not specified by default.

To do…	Use the command…	Remarks
Specify the source IP address used for the current connection	**tftp** *tftp-server* **source-ip** *ip-address* { **get** *source-file* [*dest-file*] | **put** *source-file-url* [*dest-file*] }	Optional Not specified by default.
Enter system view	**system-view**	—
Specify an interface as the source interface a TFTP client uses every time it connects to a TFTP server	**tftp source-interface** *interface-type interface-number*	Use either command Not specified by default.
Specify an IP address as the source IP address a TFTP client uses every time it connects to a TFTP server	**tftp source-ip** *ip-address*	
Display the source IP address used by a TFTP client every time it connects to a TFTP server	**display tftp source-ip**	Optional Available in any view

Note

- The specified interface must be an existing one; otherwise a prompt appears to show that the configuration fails.
- The value of the *ip-address* argument must be an IP address on the device where the configuration is performed, and otherwise a prompt appears to show that the configuration fails.
- The source interface/source IP address set for one connection is prior to the fixed source interface/source IP address set for each connection. That is, for a connection between a TFTP client and a TFTP server, if you specify the source interface/source IP address only used for the connection this time, and the specified source interface/source IP address is different from the fixed one, the former will be used for the connection this time.
- You may specify only one source interface or source IP address for the TFTP client at one time. That is, only one of the commands **tftp source-interface** and **tftp source-ip** can be effective at one time. If both commands are configured, the one configured later will overwrite the original one.

TFTP Configuration Example

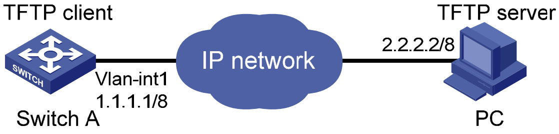
Network requirements

A switch operates as a TFTP client and a PC as the TFTP server. The application named **switch.bin** is stored on the PC. Download it (**switch.bin**) to the switch through TFTP, and use the **boot boot-loader** command to specify **switch.bin** as the application for next startup. Reboot the switch to upload the configuration file named **config.cfg** to the work directory on the PC to back up the configuration file.

- The TFTP working directory is configured on the TFTP server.
- Configure the IP addresses of a VLAN interface on the switch and the PC as 1.1.1.1 and 2.2.2.2 respectively. The port through which the switch connects with the PC belongs to the VLAN.

Network diagram

Figure 2-1 Network diagram for TFTP configurations



Configuration procedure

1) Configure the TFTP server (PC)

Start the TFTP server and configure the working directory on the PC.

2) Configure the TFTP client (switch).

Log in to the switch. (You can log in to a switch through the Console port or by telnetting the switch. See the *Login* module for detailed information.)

```
<Sysname>
```

Caution

If available space on the Flash memory of the switch is not enough to hold the file to be uploaded, you need to delete files not in use from the Flash memory to make room for the file, and then upload the file again. The files in use cannot be deleted. If you have to delete the files in use to make room for the file to be uploaded, you can only delete/download them through the Boot ROM menu.

Enter system view

```
<Sysname> system-view
[Sysname]
```

Configure the IP address of a VLAN interface on the switch to be 1.1.1.1, and ensure that the port through which the switch connects with the PC belongs to this VLAN. (This example assumes that the port belongs to VLAN 1.)

```
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address 1.1.1.1 255.255.255.0
[Sysname-Vlan-interface1] quit
```

Download the switch application named **switch.bin** from the TFTP server to the switch.

```
<Sysname> tftp 2.2.2.2 get switch.bin switch.bin
```

Upload the switch configuration file named **config.cfg** to the TFTP server.

```
<Sysname> tftp 2.2.2.2 put config.cfg config.cfg
```

After downloading the file, use the **boot boot-loader** command to specify the downloaded file (switch.bin) to be the startup file used when the switch starts the next time, and restart the switch. Thus the switch application is upgraded.

```
<Sysname> boot boot-loader switch.bin
<Sysname> reboot
```

Note

For information about the **boot boot-loader** command and how to specify the startup file for a switch, refer to the *System Maintenance and Debugging* module of this manual.

Table of Contents

1 Information Center

When configuring information center, go to these sections for information you are interested in:

- Information Center Overview
- Information Center Configuration
- Displaying and Maintaining Information Center
- Information Center Configuration Examples

Information Center Overview

Introduction to Information Center

Acting as the system information hub, information center classifies and manages system information. Together with the debugging function (the **debugging** command), information center offers a powerful support for network administrators and developers in monitoring network performance and diagnosing network problems.

The information center of the system has the following features:

Classification of system information

The system is available with three types of information:

- Log information
- Trap information
- Debugging information

Eight levels of system information

The information is classified into eight levels by severity and can be filtered by level. More emergent information has a smaller severity level.

Table 1-1 Severity description

Severity	Severity value	Description
emergencies	1	The system is unavailable.
alerts	2	Information that demands prompt reaction
critical	3	Critical information
errors	4	Error information
warnings	5	Warnings
notifications	6	Normal information that needs to be noticed
informational	7	Informational information to be recorded
debugging	8	Information generated during debugging

Information filtering by severity works this way: information with the severity value greater than the configured threshold is not output during the filtering.

- If the threshold is set to 1, only information with the severity being emergencies will be output;
- If the threshold is set to 8, information of all severities will be output.

Ten channels and six output destinations of system information

The system supports six information output destinations, including the Console, Monitor terminal (monitor), logbuffer, loghost, trapbuffer and SNMP.

The system supports ten channels. The channels 0 through 5 have their default channel names and are associated with six output destinations by default. Both the channel names and the associations between the channels and output destinations can be changed through commands.

Table 1-2 Information channels and output destinations

Information channel number	Default channel name	Default output destination
0	console	Console (Receives log, trap and debugging information.)
1	monitor	Monitor terminal (Receives log, trap and debugging information, facilitating remote maintenance.)
2	loghost	Log host (Receives log, trap and debugging information and information will be stored in files for future retrieval.)
3	trapbuffer	Trap buffer (Receives trap information, a buffer inside the device for recording information.)
4	logbuffer	Log buffer (Receives log information, a buffer inside the device for recording information.)
5	snmpagent	SNMP NMS (Receives trap information.)
6	channel6	Not specified (Receives log, trap, and debugging information.)
7	channel7	Not specified (Receives log, trap, and debugging information.)
8	channel8	Not specified (Receives log, trap, and debugging information.)
9	channel9	Not specified (Receives log, trap, and debugging information.)

Note

Configurations for the six output destinations function independently and take effect only after the information center is enabled.

Outputting system information by source module

The system information can be classified by source module and then filtered. Some module names and description are shown in Table 1-3.

Table 1-3 Source module name list

Module name	Description
8021X	802.1X module
ACL	Access control list module
ADBM	Address base module
AM	Access management module
ARP	Address resolution protocol module
CMD	Command line module
DEV	Device management module
DHCP	Dynamic host configuration protocol module
ETH	Ethernet module
FIB	Forwarding module
FTM	Fabric topology management module
FTMCMD	Fabric topology management command module
FTPS	FTP server module
HA	High availability module
HTTPD	HTTP server module
IFNET	Interface management module
IGSP	IGMP snooping module
IP	Internet protocol module
LAGG	Link aggregation module
LINE	Terminal line module
MSTP	Multiple spanning tree protocol module
NAT	Network address translation module
NDP	Neighbor discovery protocol module
NTDP	Network topology discovery protocol module
NTP	Network time protocol module
RDS	Radius module
RMON	Remote monitor module
RSA	Revest, Shamir and Adleman encryption module
SHELL	User interface module
SNMP	Simple network management protocol module
SOCKET	Socket module
SSH	Secure shell module

Module name	Description
SYSMIB	System MIB module
TAC	HWTACACS module
TELNET	Telnet module
TFTPC	TFTP client module
VLAN	Virtual local area network module
VTY	Virtual type terminal module
XM	XModem module
default	Default settings for all the modules

To sum up, the major task of the information center is to output the three types of information of the modules onto the ten channels in terms of the eight severity levels and according to the user's settings, and then redirect the system information from the ten channels to the six output destinations.

System Information Format

The format of system information varies with the output destinations.

- If the output destination is console, monitor terminal, logbuffer, trapbuffer, or SNMP, the system information is in the following format:

```
timestamp sysname module/level/digest: - unitid –content
```

Note

- The space, the forward slash /, and the colon are all required in the above format.
- Before <timestamp> may have %, “#, or * followed with a space, indicating log, alarm, or debugging information respectively.

Below is an example of the format of log information to be output to a monitor terminal:

```
%Dec  6 10:44:55:283 2006 Sysname NTP/5/NTP_LOG:- 1 - NTP service enable
```

(“-1-“ indicates that the unit number of the device is 1.)

- If the output destination is loghost, the switch and the log host use the syslog protocol. The system information is in the following format according to RFC 3164 (The BSD Syslog Protocol):

```
<Int_16>timestamp sysname %%nnmodule/level/digest: source content
```

Note

- If the address of the log host is specified in the information center of the switch, when logs are generated, the switch sends the logs to the log host in the above format. For detailed information, refer to Setting to Output System Information to a Log Host.
- There is the syslog process on the Unix or Linux platform, you can start the process to receive the logs sent from the switch; in the Windows platform, you need to install the specific software, and it will operate as the syslog host.
- Some log host software will resolve the received information as well as its format, so that the log format displayed on the log host is different from the one described in this manual.

What follows is a detailed explanation of the information fields involved:

Int_16 (Priority)

The priority is calculated using the following formula: facility*8+severity-1, in which

- facility (the device name) defaults to local7 with the value being 23 (the value of local6 is 22, that of local5 is 21, and so on).
- severity (the information level) ranges from 1 to 8. Table 1-1 details the value and meaning associated with each severity.

Note that the priority field appears only when the information has been sent to the log host.

Timestamp

The time stamp sent to the log host is in the format of Mmm dd hh:mm:ss:ms yyyy, where:

"Mmm" represents the month, and the available values are: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.

"dd" is the date, which shall follow a space if less than 10, for example, " 7".

"hh:mm:ss:ms" is the local time, where "hh" is in the 24-hour format, ranging from 00 to 23, both "mm" and "ss" range from 00 to 59, "ms" ranges from 000 to 999.

"yyyy" is the year.

Note that a space separates the time stamp and the host name.

Sysname

Sysname is the system name of the local switch and defaults to "3Com".

You can use the **sysname** command to modify the system name. Refer to the System Maintenance and Debugging part of this manual for details)

Note that there is a space between the sysname and module fields.

%%

This field is a preamble used to identify a vendor. It is displayed only when the output destination is log host.

nn

This field is a version identifier of syslog. It is displayed only when the output destination is log host.

Module

The module field represents the name of the module that generates system information. You can enter the **info-center source ?** command in system view to view the module list. Refer to Table 1-3 for module name and description.

Between "module" and "level" is a "/".

Level (Severity)

System information can be divided into eight levels based on its severity, from 1 to 8. Refer to Table 1-1 for definition and description of these severity levels. Note that there is a forward slash "/" between the level (severity) and digest fields.

Digest

The digest field is a string of up to 32 characters, outlining the system information.

Note that there is a colon between the digest and content fields.

For system information destined to the log host,

- If the character string ends with (l), it indicates the log information
- If the character string ends with (t), it indicates the trap information
- If the character string ends with (d), it indicates the debugging information

Source

This field indicates the source of the information, such as the source IP address of the log sender. This field is optional and is displayed only when the output destination is the log host.

Context

This field provides the content of the system information.

Information Center Configuration

Information Center Configuration Task List

Complete the following tasks to configure information center:

Task	Remarks
Configuring Synchronous Information Output	Optional
Configuring to Display the Time Stamp with the UTC Time Zone	Optional
Setting to Output System Information to the Console	Optional
Setting to Output System Information to a Monitor Terminal	Optional
Setting to Output System Information to a Log Host	Optional
Setting to Output System Information to the Trap Buffer	Optional
Setting to Output System Information to the Log Buffer	Optional
Setting to Output System Information to the SNMP NMS	Optional

Configuring Synchronous Information Output

Synchronous information output refers to the feature that if the system information such as log, trap, or debugging information is output when the user is inputting commands, the command line prompt (in command editing mode a prompt, or a [Y/N] string in interaction mode) and the input information are echoed after the output.

This feature is used in the case that your input is interrupted by a large amount of system output. With this feature enabled, the system echoes your previous input and you can continue your operations from where you were stopped.

Follow these steps to configure synchronous information output:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable synchronous information output	**info-center synchronous**	Required Disabled by default

Note

- If the system information is output before you input any information following the current command line prompt, the system does not echo any command line prompt after the system information output.
- In the interaction mode, you are prompted for some information input. If the input is interrupted by system output, no system prompt (except the Y/N string) will be echoed after the output, but your input will be displayed in a new line.

Configuring to Display the Time Stamp with the UTC Time Zone

To add UTC time zone to the time stamp in the information center output information, you must:

- Set the local time zone
- Set the time stamp format in the output destination of the information center to **date**
- Configure to add the UTC time zone to the output information

Follow these steps to configure to display time stamp with the UTC time zone:

<table>
<tr><th colspan="2">To do…</th><th>Use the command…</th><th>Remarks</th></tr>
<tr><td colspan="2">Set the time zone for the system</td><td>clock timezone zone-name { add | minus } time</td><td>Required
By default, UTC time zone is set for the system.</td></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td rowspan="2">Set the time stamp format in the output destination of the information center to date</td><td>Log host direction</td><td>info-center timestamp loghost date</td><td rowspan="2">Required
Use either command</td></tr>
<tr><td>Non log host direction</td><td>info-center timestamp { log | trap | debugging } date</td></tr>
</table>

To do…	Use the command…	Remarks
Set to display the UTC time zone in the output information of the information center	**info-center timestamp utc**	Required By default, no UTC time zone is displayed in the output information

Setting to Output System Information to the Console

Setting to output system information to the console

Follow these steps to set to output system information to the console:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable system information output to the console	**info-center console channel** { *channel-number* | *channel-name* }	Optional By default, the switch uses information channel 0 to output log/debugging/trap information to the console.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp { log | trap | debugging } { boot | date | none }**	Optional By default, the time stamp format of the log and trap output information is **date**, and that of the debugging output information is **boot**.

Note

To view the debugging information of some modules on the switch, you need to set the type of the output information to **debug** when configuring the system information output rules, and use the **debugging** command to enable debugging for the corresponding modules.

Table 1-4 Default output rules for different output destinations

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/disabled	Severity	Enabled/disabled	Severity	Enabled/disabled	Severity
Console	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging

Output destination	Modules allowed	LOG		TRAP		DEBUG	
		Enabled/disabled	Severity	Enabled/disabled	Severity	Enabled/disabled	Severity
Monitor terminal	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Log host	default (all modules)	Enabled	informational	Enabled	debugging	Disabled	debugging
Trap buffer	default (all modules)	Disabled	informational	Enabled	warnings	Disabled	debugging
Log buffer	default (all modules)	Enabled	warnings	Disabled	debugging	Disabled	debugging
SNMP NMS	default (all modules)	Disabled	debugging	Enabled	warnings	Disabled	debugging

Enabling system information display on the console

After setting to output system information to the console, you need to enable the associated display function to display the output information on the console.

Follow these steps to enable the system information display on the console:

To do…	Use the command…	Remarks
Enable the debugging/log/trap information terminal display function	**terminal monitor**	Optional Enabled by default.
Enable debugging information terminal display function	**terminal debugging**	Optional Disabled by default.
Enable log information terminal display function	**terminal logging**	Optional Enabled by default.
Enable trap information terminal display function	**terminal trapping**	Optional Enabled by default.

Note

Make sure that the debugging/log/trap information terminal display function is enabled (use the **terminal monitor** command) before you enable the corresponding terminal display function by using the **terminal debugging**, **terminal logging**, or **terminal trapping** command.

Setting to Output System Information to a Monitor Terminal

System information can also be output to a monitor terminal, which is a user terminal that has login connections through the AUX, or VTY user interface.

Setting to output system information to a monitor terminal

Follow these steps to set to output system information to a monitor terminal:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable system information output to Telnet terminal or dumb terminal	**info-center monitor channel** { *channel-number* | *channel-name* }	Optional By default, a switch outputs log/debugging/trap information to a user terminal through information channel 1.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional By default, the time stamp format of the log and trap output information is **date**, and that of the debugging output information is **boot**.

Note

- When there are multiple Telnet users or dumb terminal users, they share some configuration parameters including module filter, language and severity level threshold. In this case, change to any such parameter made by one user will also be reflected on all other user terminals.
- To view debugging information of specific modules, you need to set the information type as **debug** when setting the system information output rules, and enable debugging for corresponding modules through the **debugging** command.

Enabling system information display on a monitor terminal

After setting to output system information to a monitor terminal, you need to enable the associated display function in order to display the output information on the monitor terminal.

Follow these steps to enable the display of system information on a monitor terminal:

To do…	Use the command…	Remarks
Enable the debugging/log/trap information terminal display function	**terminal monitor**	Optional Enabled by default
Enable debugging information terminal display function	**terminal debugging**	Optional Disabled by default
Enable log information terminal display function	**terminal logging**	Optional Enabled by default

To do…	Use the command…	Remarks
Enable trap information terminal display function	**terminal trapping**	Optional Enabled by default

Note

Make sure that the debugging/log/trap information terminal display function is enabled (use the **terminal monitor** command) before you enable the corresponding terminal display function by using the **terminal debugging**, **terminal logging**, or **terminal trapping** command.

Setting to Output System Information to a Log Host

Follow these steps to set to output system information to a log host:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable information output for a specified switch in a fabric	**info-center switch-on** { **unit** *unit-id* | **master** | **all** } [**debugging** | **logging** | **trapping**]*	Optional By default, debugging information output is enabled, and log and trap information output are disabled for the master switch in a fabric. Debugging, log and trap information output are all disabled for other switches in the fabric.
Enable system information output to a log host	**info-center loghost** *host-ip-addr* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number*]*	Required By default, the switch does not output information to the log host. After you configure the switch to output information to the log host, the switch uses information channel 2 by default.
Configure the source interface through which log information is sent to the log host	**info-center loghost source** *interface-type interface-number*	Optional By default, no source interface is configured, and the system automatically selects an interface as the source interface.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of the time stamp to be sent to the log host	**info-center timestamp loghost** { **date** | **no-year-date** | **none** }	Optional By default, the time stamp format of the information output to the log host is **date**.

Note

- After the switches form a fabric, you can use the **info-center switch-on** command to enable the information output for the switches to make the log, debugging and trap information of each switch in the fabric synchronous. Each switch sends its own information to other switches in the fabric and receives information sent by other switches at the same time to update the information on itself. In this way, the switch ensures the synchronization of log, debugging and trap information in the whole fabric.
- Be sure to set the correct IP address when using the **info-center loghost** command. A loopback IP address will cause an error message prompting that this address is invalid.

Setting to Output System Information to the Trap Buffer

Follow these steps to set to output system information to the trap buffer:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable system information output to the trap buffer	**info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*	Optional By default, the switch uses information channel 3 to output trap information to the trap buffer, which can holds up to 256 items by default.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional By default, the time stamp format of the output trap information is **date**.

Setting to Output System Information to the Log Buffer

Follow these steps to set to output system information to the log buffer:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.

To do…	Use the command…	Remarks
Enable information output to the log buffer	**info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*]*	Optional By default, the switch uses information channel 4 to output log information to the log buffer, which can holds up to 512 items by default.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional By default, the time stamp format of the output log information is **date**.

Setting to Output System Information to the SNMP NMS

Follow these steps to set to output system information to the SNMP NMS:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable the information center	**info-center enable**	Optional Enabled by default.
Enable information output to the SNMP NMS	**info-center snmp channel** { *channel-number* | *channel-name* }	Optional By default, the switch outputs trap information to SNMP through channel 5.
Configure the output rules of system information	**info-center source** { *modu-name* | **default** } **channel** { *channel-number* | *channel-name* } [{ **log** | **trap** | **debug** } { **level** *severity* | **state** *state* }]*	Optional Refer to Table 1-4 for the default output rules of system information.
Set the format of time stamp in the output information	**info-center timestamp** { **log** | **trap** | **debugging** } { **boot** | **date** | **none** }	Optional By default, the time stamp format of the information output to the SNMP NMS is **date**.

Note

To send information to a remote SNMP NMS properly, related configurations are required on both the switch and the SNMP NMS. For the detailed configuration, refer to the *SNMP-RMON* part.

Displaying and Maintaining Information Center

To do…	Use the command…	Remarks
Display information on an information channel	**display channel** [*channel-number* | *channel-name*]	Available in any view
Display the operation status of information center, the configuration of information channels, the format of time stamp and the information output in case of fabric	**display info-center** [**unit** *unit-id*]	
Display the status of log buffer and the information recorded in the log buffer	**display logbuffer** [**unit** *unit-id*] [**level** *severity* | **size** *buffersize*]* [| { **begin** | **exclude** | **include** } *regular-expression*]	
Display the summary information recorded in the log buffer	**display logbuffer summary** [**level** *severity*]	
Display the status of trap buffer and the information recorded in the trap buffer	**display trapbuffer** [**unit** *unit-id*] [**size** *buffersize*]	
Clear information recorded in the log buffer	**reset logbuffer** [**unit** *unit-id*]	Available in user view
Clear information recorded in the trap buffer	**reset trapbuffer** [**unit** *unit-id*]	

Information Center Configuration Examples

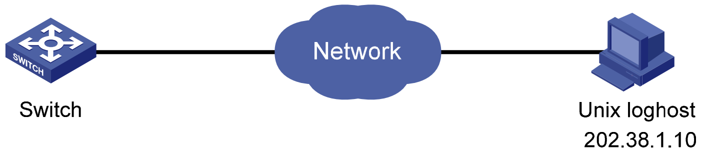
Log Output to a UNIX Log Host

Network requirements

The switch sends the following log information to the Unix log host whose IP address is 202.38.1.10: the log information of the two modules ARP and IP, with severity higher than "informational".

Network diagram

Figure 1-1 Network diagram for log output to a Unix log host



Configuration procedure

1) Configure the switch:

Enable the information center.

```
<Switch> system-view
[Switch] info-center enable
```

Disable the function of outputting information to log host channels, because all modules output log information to the log host channels by default.

```
[Switch] undo info-center source default channel loghost
```

Configure the host whose IP address is 202.38.1.10 as the log host. Permit ARP and IP modules to output information with severity level higher than informational to the log host.

```
[Switch] info-center loghost 202.38.1.10 facility local4
[Switch] info-center source arp channel loghost log level informational debug state off trap
state off
[Switch] info-center source ip channel loghost log level informational debug state off trap
state off
```

2) Configure the log host:

The operations here are performed on SunOS 4.0. The operations on other manufacturers' Unix operation systems are similar.

Step 1: Execute the following commands as the super user (root user).

```
# mkdir /var/log/Switch
# touch /var/log/Switch/information
```

Step 2: Edit the file "/etc/syslog.conf" as the super user (root user) to add the following selector/action pairs.

```
# Switch configuration messages
local4.info	/var/log/Switch/information
```

Note

When you edit the file "/etc/syslog.conf", note that:

- A note must start in a new line, starting with a "#" sign.
- In each pair, a tab should be used as a separator instead of a space.
- No space is allowed at the end of a file name.
- The device name (facility) and received log information severity level specified in the file "/etc/syslog.conf" must be the same as those corresponding parameters configured in the commands **info-center loghost** and **info-center source**. Otherwise, log information may not be output to the log host normally.

Step 3: After the log file "information" is created and the file "/etc/syslog.conf" is modified, execute the following command to send a HUP signal to the system daemon "syslogd", so that it can reread its configuration file "/etc/syslog.conf".

```
# ps -ae | grep syslogd
147
# kill -HUP 147
```

After all the above operations, the switch can make records in the corresponding log file.

Note

Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and the file “syslog.conf”, you can sort information precisely for filtering.

Log Output to a Linux Log Host

Network requirements

The switch sends the following log information to the Linux log host whose IP address is 202.38.1.10: All modules' log information, with severity higher than “errors”.

Network diagram

Figure 1-2 Network diagram for log output to a Linux log host

Configuration procedure

1) Configure the switch:

Enable the information center.

```
<Switch> system-view
[Switch] info-center enable
```

Configure the host whose IP address is 202.38.1.10 as the log host. Permit all modules to output log information with severity level higher than error to the log host.

```
[Switch] info-center loghost 202.38.1.10 facility local7
[Switch] info-center source default channel loghost log level errors debug state off trap
state off
```

2) Configure the log host:

Step 1: Execute the following commands as a super user (root user).

```
# mkdir /var/log/Switch
# touch /var/log/Switch/information
```

Step 2: Edit the file “/etc/syslog.conf” as the super user (root user) to add the following selector/action pairs.

```
# Switch configuration messages
local7.info     /var/log/Switch/information
```

Note

Note the following items when you edit file “/etc/syslog.conf”.

- A note must start in a new line, starting with a “#" sign.
- In each pair, a tab should be used as a separator instead of a space.
- No space is permitted at the end of the file name.
- The device name (facility) and received log information severity specified in file “/etc/syslog.conf” must be the same with those corresponding parameters configured in commands **info-center loghost** and **info-center source**. Otherwise, log information may not be output to the log host normally.

Step 3: After the log file “information” is created and the file “/etc/syslog.conf” is modified, execute the following commands to view the process ID of the system daemon “syslogd”, stop the process, and then restart the daemon "syslogd" in the background with the “-r” option.

```
# ps -ae | grep syslogd
147
# kill -9 147
# syslogd -r &
```

In case of Linux log host, the daemon “syslogd” must be started with the “-r” option.

After all the above operations, the switch can record information in the corresponding log file.

Note

Through combined configuration of the device name (facility), information severity level threshold (severity), module name (filter) and the file “syslog.conf”, you can sort information precisely for filtering.

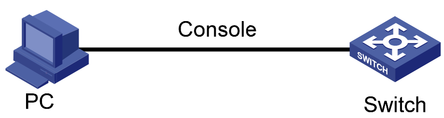
Log Output to the Console

Network requirements

The switch sends the following information to the console: the log information of the two modules ARP and IP, with severity higher than “informational”.

Network diagram

Figure 1-3 Network diagram for log output to the console



Configuration procedure

Enable the information center.

```
<Switch> system-view
[Switch] info-center enable
```

Disable the function of outputting information to the console channels.

```
[Switch] undo info-center source default channel console
```

Enable log information output to the console. Permit ARP and IP modules to output log information with severity level higher than informational to the console.

```
[Switch] info-center console channel console
[Switch] info-center source arp channel console log level informational debug state off trap state off
[Switch] info-center source ip channel console log level informational debug state off trap state off
```

Enable terminal display.

```
<Switch> terminal monitor
<Switch> terminal logging
```

Configuration Example

Network requirements

- The switch is in the time zone of GMT+ 08:00:00.
- The time stamp format of output log information is date.
- UTC time zone will be added to the output information of the information center.

Network diagram

Figure 1-4 Network diagram

Configuration procedure

Name the local time zone z8 and configure it to be eight hours ahead of UTC time.

```
<Switch> clock timezone z8 add 08:00:00
```

Set the time stamp format of the log information to be output to the log host to date.

```
<Switch> system-view
System View: return to User View with Ctrl+Z.
[Switch] info-center timestamp loghost date
```

Configure to add UTC time to the output information of the information center.

```
[Switch] info-center timestamp utc
```

Table of Contents

1 Boot ROM and Host Software Loading

Traditionally, switch software is loaded through a serial port. This approach is slow, time-consuming and cannot be used for remote loading. To resolve these problems, the TFTP and FTP modules are introduced into the switch. With these modules, you can load/download software/files conveniently to the switch through an Ethernet port.

This chapter introduces how to load the Boot ROM and host software to a switch locally and remotely.

When configuring the Boot ROM and host software loading, go to these sections for information you are interested in:

- Introduction to Loading Approaches
- Local Boot ROM and Software Loading
- Remote Boot ROM and Software Loading

Introduction to Loading Approaches

You can load software locally by using:

- XModem through Console port
- TFTP through Ethernet port
- FTP through Ethernet port

You can load software remotely by using:

- FTP
- TFTP

Note

The Boot ROM software version should be compatible with the host software version when you load the Boot ROM and host software.

Local Boot ROM and Software Loading

If your terminal is directly connected to the Console port of the switch, you can load the Boot ROM and host software locally.

Before loading the software, make sure that your terminal is correctly connected to the switch.

Note

The loading process of the Boot ROM software is the same as that of the host software, except that during the former process, you should press "6" or <Ctrl+U> and <Enter> after entering the BOOT menu and the system gives different prompts. The following text mainly describes the Boot ROM loading process.

BOOT Menu

```
Starting......



      ****************************************************************
      *                                                              *
      *             Switch 4500 26-Port BOOTROM, Version 3.01        *
      *                                                              *
      ****************************************************************

      Copyright (c) 2004-2008 3Com Corporation and its licensors.
      Creation date   : Sep  8 2008, 14:35:39
      CPU Clock Speed : 200MHz
      BUS Clock Speed : 33MHz
      Memory Size     : 64MB

      Mac Address     : 00e0fc003962


Press Ctrl-B to enter Boot Menu...
```

Press <Ctrl+B>. The system displays:

```
Password :
```

Note

To enter the BOOT menu, you should press <Ctrl+B> within five seconds (full startup mode) or one second (fast startup mode) after the information "Press Ctrl-B to enter BOOT Menu..." displays. Otherwise, the system starts to extract the program; and if you want to enter the BOOT Menu at this time, you will have to restart the switch.

Enter the correct Boot ROM password (no password is set by default). The system enters the BOOT Menu:

```
             BOOT  MENU
```

```
1. Download application file to flash
2. Select application file to boot
3. Display all files in flash
4. Delete file from flash
5. Modify bootrom password
6. Enter bootrom upgrade menu
7. Skip current configuration file
8. Set bootrom password recovery
9. Set switch startup mode
0. Reboot

Enter your choice(0-9):
```

Loading by XModem through Console Port

Introduction to XModem

XModem protocol is a file transfer protocol that is widely used due to its simplicity and high stability. The XModem protocol transfers files through Console port. It supports two types of data packets (128 bytes and 1 KB), two check methods (checksum and CRC), and multiple attempts of error packet retransmission (generally the maximum number of retransmission attempts is ten).

The XModem transmission procedure is completed by a receiving program and a sending program. The receiving program sends negotiation characters to negotiate a packet checking method. After the negotiation, the sending program starts to transmit data packets. When receiving a complete packet, the receiving program checks the packet using the agreed method. If the check succeeds, the receiving program sends acknowledgement characters and the sending program proceeds to send another packet. If the check fails, the receiving program sends negative acknowledgement characters and the sending program retransmits the packet.

Loading Boot ROM

Follow these steps to load the Boot ROM:

Step 1: At the prompt "Enter your choice(0-9):" in the BOOT Menu, press <6> or <Ctrl+U>, and then press <Enter> to enter the Boot ROM update menu shown below:

```
Bootrom update menu:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

Step 2: Press 3 in the above menu to download the Boot ROM using XModem. The system displays the following setting menu for download baudrate:

```
Please select your download baudrate:
1.* 9600
2. 19200
3. 38400
4. 57600
5. 115200
```

```
0. Return

Enter your choice (0-5):
```

Step 3: Choose an appropriate baudrate for downloading. For example, if you press 5, the baudrate 115200 bps is chosen and the system displays the following information:

```
Download baudrate is 115200 bit/s
Please change the terminal's baudrate to 115200 bit/s and select XMODEM protocol
Press enter key when ready
```

Note

If you have chosen 9600 bps as the download baudrate, you need not modify the HyperTerminal's baudrate, and therefore you can skip Step 4 and 5 below and proceed to Step 6 directly. In this case, the system will not display the above information.

Following are configurations on PC. Take the HyperTerminal in Windows 2000 as an example.

Step 4: Choose [File/Properties] in HyperTerminal, click <Configure> in the pop-up dialog box, and then select the baudrate of 115200 bps in the Console port configuration dialog box that appears, as shown in Figure 1-1, Figure 1-2.

Figure 1-1 Properties dialog box

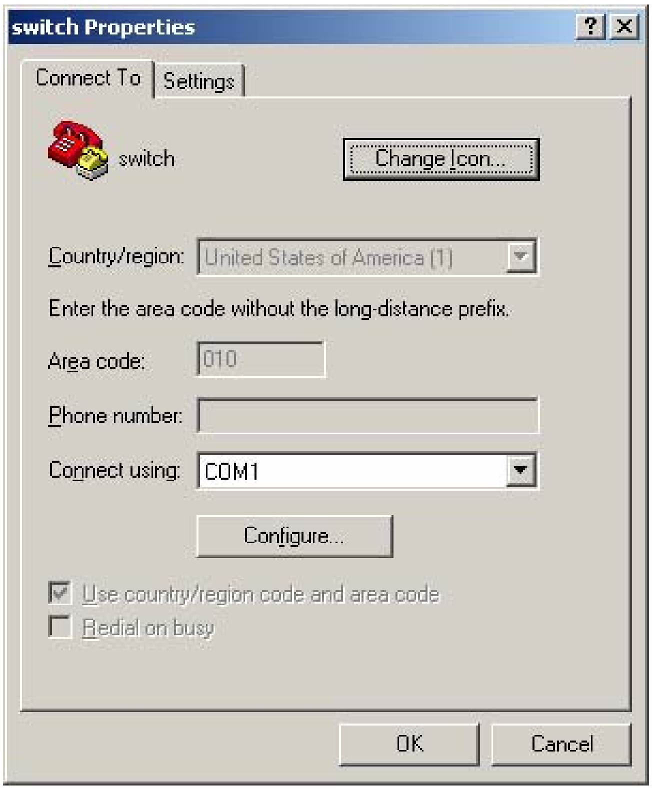
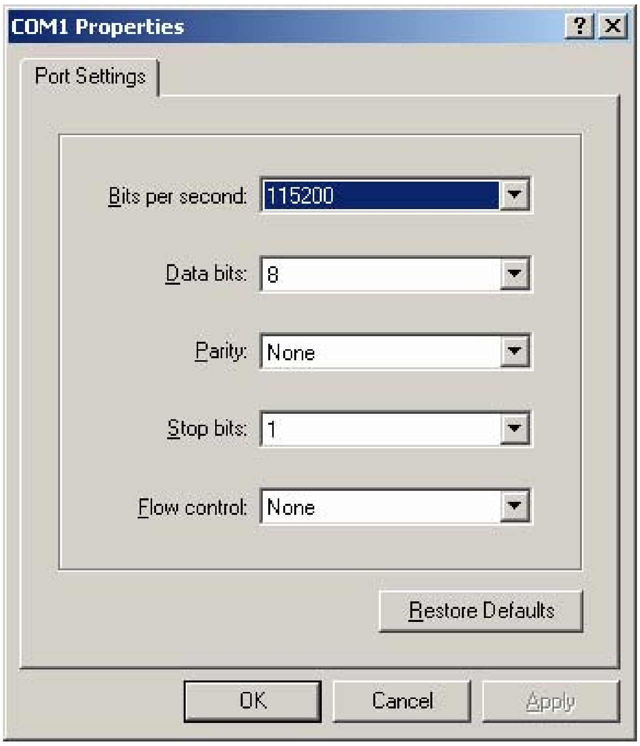
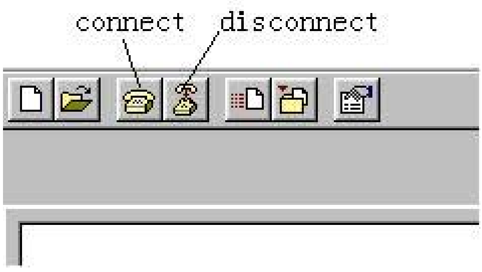


Figure 1-2 Console port configuration dialog box



Step 5: Click the <Disconnect> button to disconnect the HyperTerminal from the switch and then click the <Connect> button to reconnect the HyperTerminal to the switch, as shown in Figure 1-3.

Figure 1-3 Connect and disconnect buttons



Note

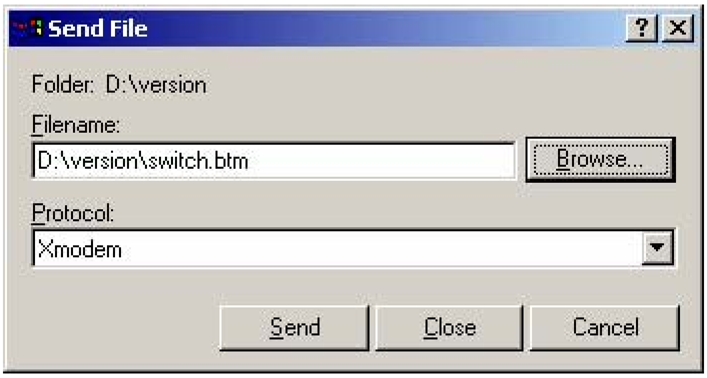
The new baudrate takes effect after you disconnect and reconnect the HyperTerminal program.

Step 6: Press <Enter> to start downloading the program. The system displays the following information:

```
Now please start transfer file with XMODEM protocol.
If you want to exit, Press <Ctrl+X>.
Loading ...CCCCCCCCCC
```

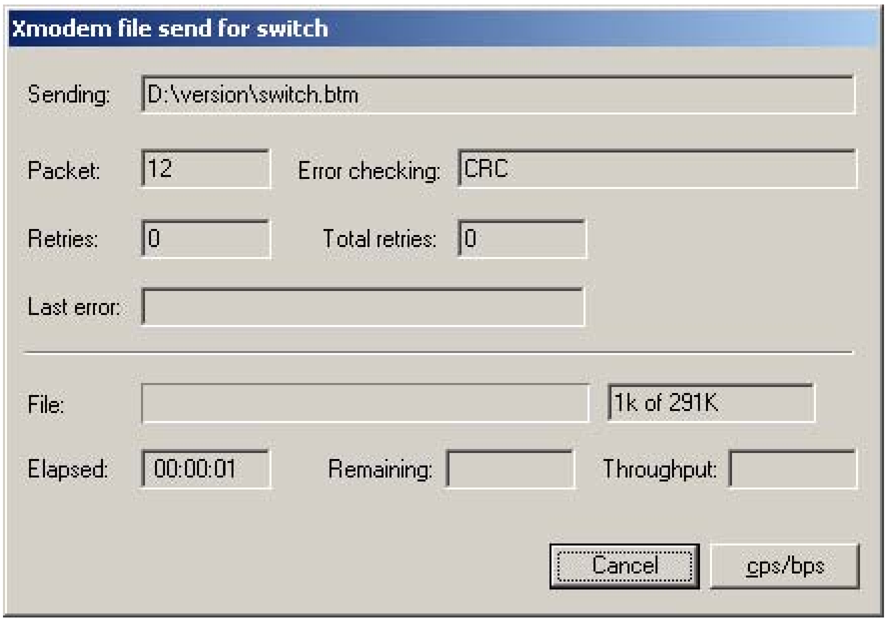
Step 7: Choose [Transfer/Send File] in HyperTerminal, and click <Browse> in pop-up dialog box, as shown in Figure 1-4. Select the software file that you need to load to the switch, and set the protocol to XModem.

Figure 1-4 Send file dialog box



Step 8: Click <Send>. The system displays the page, as shown in Figure 1-5.

Figure 1-5 Sending file page



Step 9: After the sending process completes, the system displays the following information:

```
Loading ...CCCCCCCCCC done!
```

Step 10: Reset HyperTerminal's baudrate to 9600 bps (refer to Step 4 and 5). Then, press any key as prompted. The system will display the following information when it completes the loading.

```
Bootrom updating...................................done!
```

Note

- If the HyperTerminal's baudrate is not reset to 9600 bps, the system prompts "Your baudrate should be set to 9600 bps again! Press enter key when ready".
- You need not reset the HyperTerminal's baudrate and can skip the last step if you have chosen 9600 bps. In this case, the system upgrades the Boot ROM automatically and prompts "Bootrom updating now...................................done!".

Loading host software

Follow these steps to load the host software:

Step 1: Select <1> in BOOT Menu and press <Enter>. The system displays the following information:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

Step 2: Enter 3 in the above menu to load the host software by using XModem.

The subsequent steps are the same as those for loading the Boot ROM, except that the system gives the prompt for host software loading instead of Boot ROM loading.

Note

You can also use the **xmodem get** command to load host software through the Console port (of AUX type). The load procedures are as follows (assume that the PC is connected to the Console port of the switch, and logs onto the switch through the Console port):

Step 1: Execute the **xmodem get** command in user view. In this case, the switch is ready to receive files.

Step 2: Enable the HyperTerminal on the PC, and configure XModem as the transfer protocol, and configure communication parameters on the Hyper Terminal the same as that on the Console port.

Step 3: Choose the file to be loaded to the switch, and then start to transmit the file.

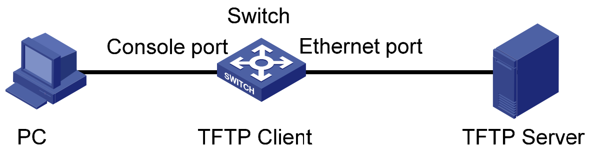
Loading by TFTP through Ethernet Port

Introduction to TFTP

TFTP, a protocol in TCP/IP protocol suite, is used for trivial file transfer between client and server. It is over UDP to provide unreliable data stream transfer service.

Loading the Boot ROM

Figure 1-6 Local loading using TFTP



Step 1: As shown in Figure 1-6, connect the switch through an Ethernet port to the TFTP server, and connect the switch through the Console port to the configuration PC.

Note

You can use one PC as both the configuration device and the TFTP server.

Step 2: Run the TFTP server program on the TFTP server, and specify the path of the program to be downloaded.

Caution

TFTP server program is not provided with the 3Com Series Ethernet Switches.

Step 3: Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the BOOT Menu.

At the prompt "Enter your choice(0-9):" in the BOOT Menu, press <6> or <Ctrl+U>, and then press <Enter> to enter the Boot ROM update menu shown below:

```
Bootrom update menu:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

Step 4: Enter 1 in the above menu to download the Boot ROM using TFTP. Then set the following TFTP-related parameters as required:

```
Load File name          :Switch.btm
Switch IP address       :1.1.1.2
Server IP address       :1.1.1.1
```

Step 5: Press <Enter>. The system displays the following information:

```
Are you sure to update your bootrom?Yes or No(Y/N)
```

Step 6: Enter Y to start file downloading or N to return to the Boot ROM update menu. If you enter Y, the system begins to download and update the Boot ROM. Upon completion, the system displays the following information:

```
Loading........................................done
Bootrom updating..........done!
```

Loading host software

Follow these steps to load the host software.

Step 1: Select <1> in BOOT Menu and press <Enter>. The system displays the following information:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
```

```
0. Return to boot menu

Enter your choice(0-3):
```

Step 2: Enter 1 in the above menu to download the host software using TFTP.

The subsequent steps are the same as those for loading the Boot ROM, except that the system gives the prompt for host software loading instead of Boot ROM loading.

Caution

When loading Boot ROM and host software using TFTP through BOOT menu, you are recommended to use the PC directly connected to the device as TFTP server to promote upgrading reliability.

Loading by FTP through Ethernet Port

Introduction to FTP

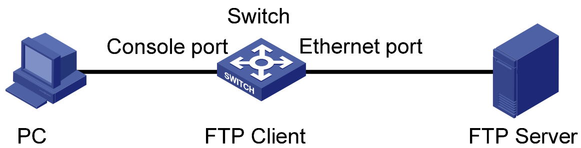
FTP is an application-layer protocol in the TCP/IP protocol suite. It is used for file transfer between server and client, and is widely used in IP networks.

You can use the switch as an FTP client or a server, and download software to the switch through an Ethernet port. The following is an example.

Loading Procedure Using FTP Client

- Loading Boot ROM

Figure 1-7 Local loading using FTP client



Step 1: As shown in Figure 1-7, connect the switch through an Ethernet port to the FTP server, and connect the switch through the Console port to the configuration PC.

Note

You can use one computer as both configuration device and FTP server.

Step 2: Run the FTP server program on the FTP server, configure an FTP user name and password, and copy the program file to the specified FTP directory.

Step 3: Run the HyperTerminal program on the configuration PC. Start the switch. Then enter the BOOT Menu.

At the prompt "Enter your choice(0-9):" in the BOOT Menu, press <6> or <Ctrl+U>, and then press <Enter> to enter the Boot ROM update menu shown below:

```
Bootrom update menu:
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

Step 4: Enter 2 in the above menu to download the Boot ROM using FTP. Then set the following FTP-related parameters as required:

```
Load File name          :switch.btm
Switch IP address       :10.1.1.2
Server IP address       :10.1.1.1
FTP User Name           :Switch
FTP User Password       :abc
```

Step 5: Press <Enter>. The system displays the following information:

```
Are you sure to update your bootrom?Yes or No(Y/N)
```

Step 6: Enter Y to start file downloading or N to return to the Boot ROM update menu. If you enter Y, the system begins to download and update the program. Upon completion, the system displays the following information:

```
Loading.......................................done
Bootrom updating.........done!
```

- Loading host software

Follow these steps to load the host software:

Step 1: Select <1> in BOOT Menu and press <Enter>. The system displays the following information:

```
1. Set TFTP protocol parameter
2. Set FTP protocol parameter
3. Set XMODEM protocol parameter
0. Return to boot menu

Enter your choice(0-3):
```

Enter 2 in the above menu to download the host software using FTP.

The subsequent steps are the same as those for loading the Boot ROM, except for that the system gives the prompt for host software loading instead of Boot ROM loading.

Caution

When loading the Boot ROM and host software using FTP through BOOT menu, you are recommended to use the PC directly connected to the device as FTP server to promote upgrading reliability.

Remote Boot ROM and Software Loading

If your terminal is not directly connected to the switch, you can telnet to the switch, and use FTP or TFTP to load the Boot ROM and host software remotely.

Remote Loading Using FTP

Loading Procedure Using FTP Client

1) Loading the Boot ROM

As shown in Figure 1-8, a PC is used as both the configuration device and the FTP server. You can telnet to the switch, and then execute the FTP commands to download the Boot ROM program switch.btm from the remote FTP server (whose IP address is 10.1.1.1) to the switch.

Figure 1-8 Remote loading using FTP Client

Step 1: Download the program to the switch using FTP commands.

```
<Sysname> ftp 10.1.1.1
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):abc
331 Give me your password, please
Password:
230 Logged in successfully
[ftp] get switch.btm
[ftp] bye
```

Note

When using different FTP server software on PC, different information will be output to the switch.

Step 2: Update the Boot ROM program on the switch.

```
<Sysname> boot bootrom switch.btm
 This will update BootRom file on unit 1. Continue? [Y/N] y
 Upgrading BOOTROM, please wait...
 Upgrade BOOTROM succeeded!
```

Step 3: Restart the switch.

```
<Sysname> reboot
```

Note

Before restarting the switch, make sure you have saved all other configurations that you want, so as to avoid losing configuration information.

2) Loading host software

Loading the host software is the same as loading the Boot ROM program, except that the file to be downloaded is the host software file, and that you need to use the **boot boot-loader** command to select the host software used for next startup of the switch.

After the above operations, the Boot ROM and host software loading is completed.

Pay attention to the following:

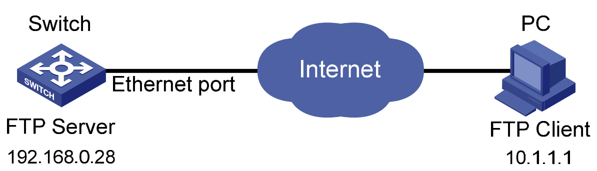
- The loading of Boot ROM and host software takes effect only after you restart the switch with the **reboot** command.
- If the space of the Flash memory is not enough, you can delete the unused files in the Flash memory before software downloading. For information about deleting files, refer to *File System Management* part of this manual.
- Ensure the power supply during software loading.

Loading Procedure Using FTP Server

As shown in Figure 1-9, the switch is used as the FTP server. You can telnet to the switch, and then execute the FTP commands to upload the Boot ROM switch.btm to the switch.

1) Loading the Boot ROM

Figure 1-9 Remote loading using FTP server



Step 1: As shown in Figure 1-9, connect the switch through an Ethernet port to the PC (whose IP address is 10.1.1.1)

Step 2: Configure the IP address of VLAN-interface 1 on the switch to 192.168.0.28, and subnet mask to 255.255.255.0.

Note

You can configure the IP address for any VLAN on the switch for FTP transmission. However, before configuring the IP address for a VLAN interface, you have to make sure whether the IP addresses of this VLAN and PC are routable.

```
<Sysname> system-view
```

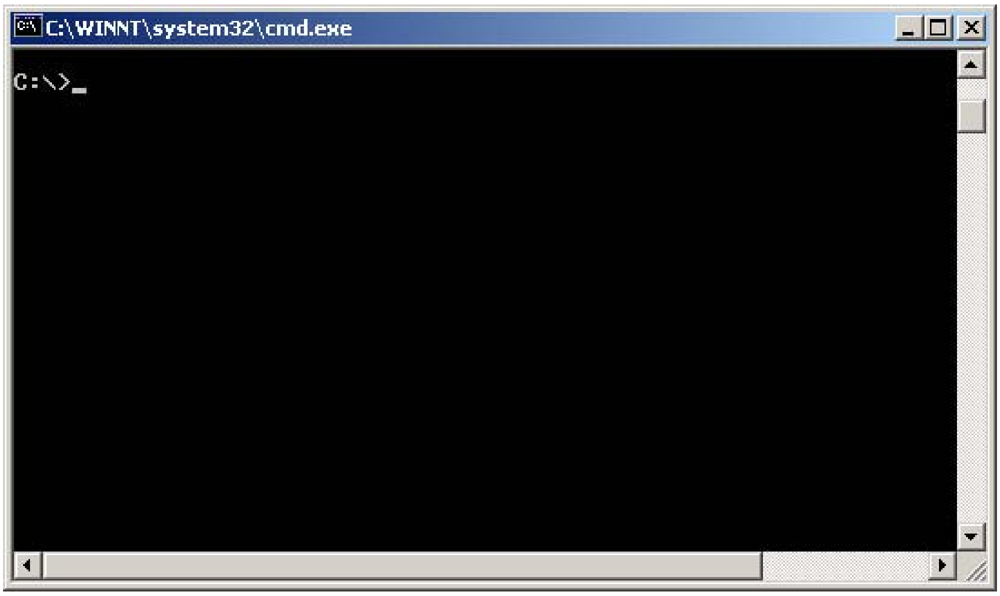
```
System View: return to User View with Ctrl+Z.
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address 192.168.0.28 255.255.255.0
```

Step 3: Enable FTP service on the switch, and configure the FTP user name to test and password to pass.

```
[Sysname-Vlan-interface1] quit
[Sysname] ftp server enable
[Sysname] local-user test
New local user added.
[Sysname-luser-test] password simple pass
[Sysname-luser-test] service-type ftp
```

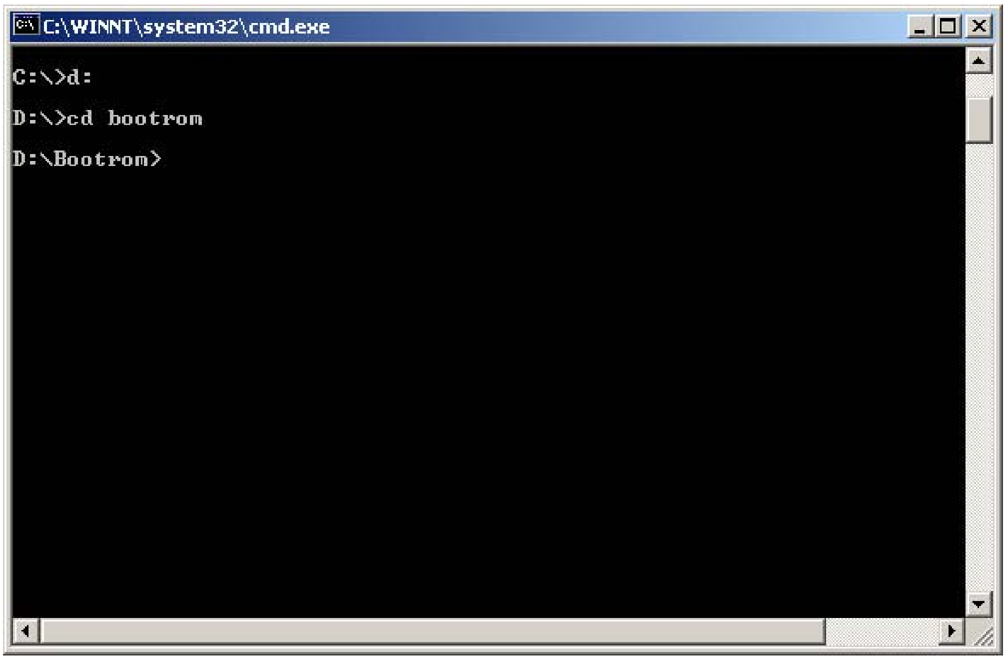
Step 4: Enable FTP client software on the PC. Refer to Figure 1-10 for the command line interface in Windows operating system.

Figure 1-10 Command line interface



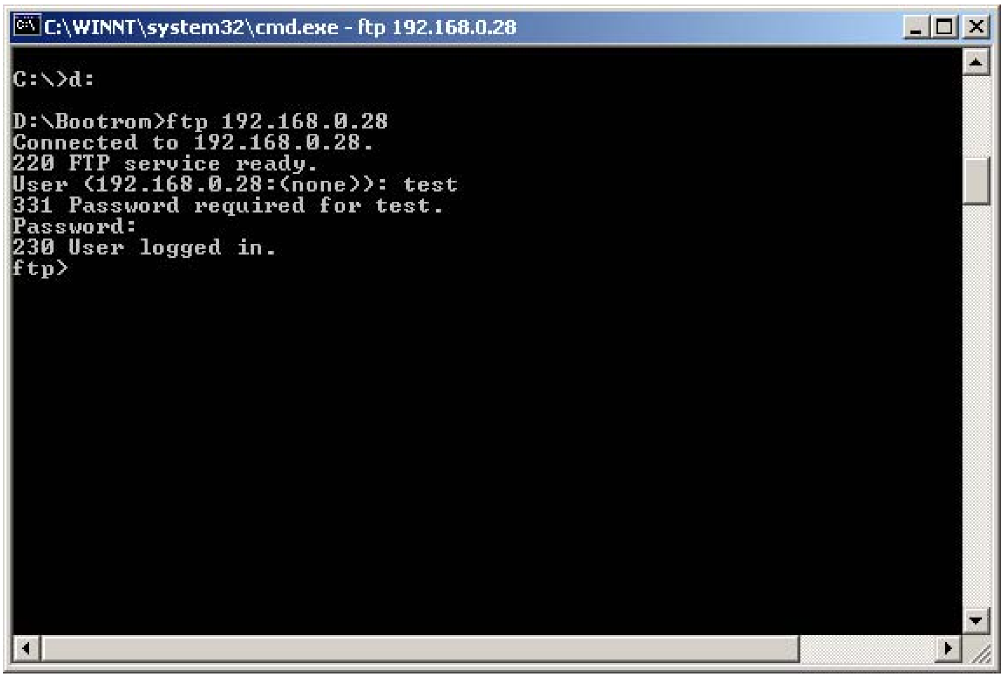
Step 5: Use the **cd** command on the interface to enter the path that the Boot ROM upgrade file is to be stored. Assume the name of the path is D:\Bootrom, as shown in Figure 1-11.

Figure 1-11 Enter Boot ROM directory



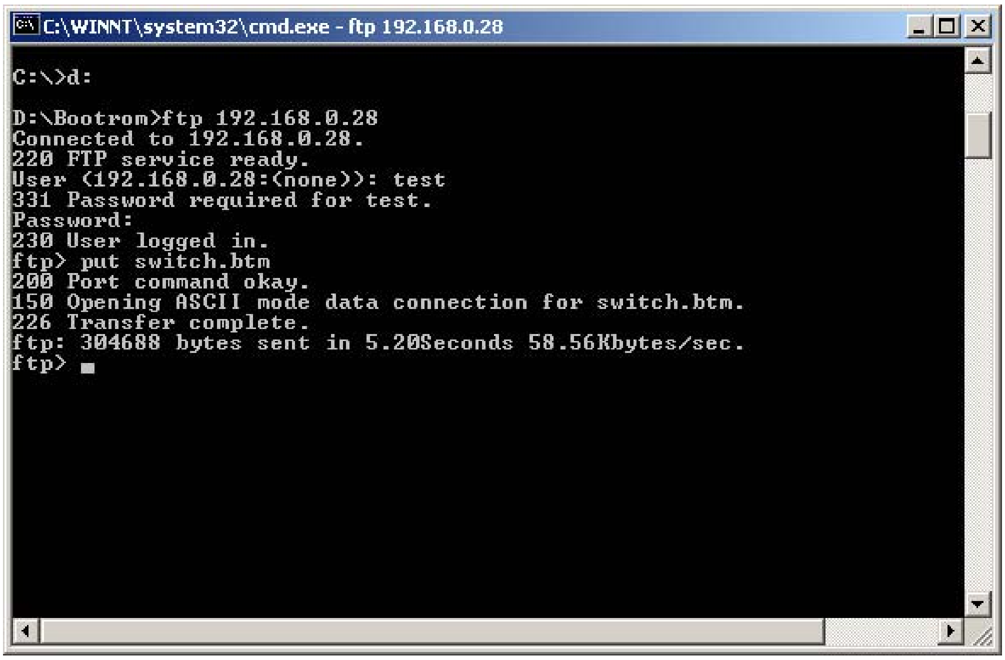
Step 6: Enter **ftp 192.168.0.28** and enter the user name **test**, password **pass**, as shown in Figure 1-12, to log on to the FTP server.

Figure 1-12 Log on to the FTP server



Step 7: Use the **put** command to upload the file switch.btm to the switch, as shown in Figure 1-13.

Figure 1-13 Upload file switch.btm to the switch



Step 8: Configure switch.btm to be the Boot ROM at next startup, and then restart the switch.

```
<Sysname> boot bootrom switch.btm
 This will update Bootrom on unit 1.  Continue? [Y/N] y
 Upgrading Bootrom, please wait...
 Upgrade Bootrom succeeded!
<Sysname> reboot
```

After the switch restarts, the file switch.btm is used as the Boot ROM. It indicates that the Boot ROM loading is finished.

2) Loading host software

Loading the host software is the same as loading the Boot ROM program, except that the file to be downloaded is the host software file, and that you need to use the **boot boot-loader** command to select the host software used for the next startup of the switch.

Note

- The steps listed above are performed in the Windows operating system, if you use other FTP client software, refer to the corresponding user guide before operation.
- Only the configuration steps concerning loading are listed here. For detailed description on the corresponding configuration commands, refer to *FTP-SFTP-TFTP* part of this manual.

Remote Loading Using TFTP

The remote loading using TFTP is similar to that using FTP. The only difference is that TFTP is used to load software to the switch, and the switch can only act as a TFTP client.

2 Basic System Configuration and Debugging

When configuring basic system configuration and debugging, go to these sections for information you are interested in:

- Basic System Configuration
- Displaying the System Status
- Debugging the System

Basic System Configuration

Perform the following basic system configuration:

To do…	Use the command…	Remarks
Set the current date and time of the system	**clock datetime** *HH:MM:SS* { *YYYY/MM/DD* | *MM/DD/YYYY* }	Required Execute this command in user view. The default value is 23:55:00 04/01/2000 when the system starts up.
Set the local time zone	**clock timezone** *zone-name* { **add** | **minus** } *HH:MM:SS*	Optional Execute this command in user view. By default, it is the UTC time zone.
Set the name and time range of the summer time	**clock summer-time** *zone_name* { **one-off** | **repeating** } *start-time start-date end-time end-date offset-time*	Optional Execute this command in user view. • When the system reaches the specified start time, it automatically adds the specified offset to the current time, so as to toggle the system time to the summer time. • When the system reaches the specified end time, it automatically subtracts the specified offset from the current time, so as to toggle the summer time to normal system time.
Enter system view from user view	**system-view**	—
Set the system name of the switch	**sysname** *sysname*	Optional By default, the name is 3Com.
Return from current view to lower level view	**quit**	Optional If the current view is user view, you will quit the current user interface.
Return from current view to user view	**return**	Optional The composite key <Ctrl+Z> has the same effect with the **return** command.

Displaying the System Status

To do…	Use the command…	Remarks
Display the current date and time of the system	**display clock**	Available in any view
Display the version of the system	**display version**	
Display the information about users logging onto the switch	**display users** [**all**]	

Debugging the System

Enabling/Disabling System Debugging

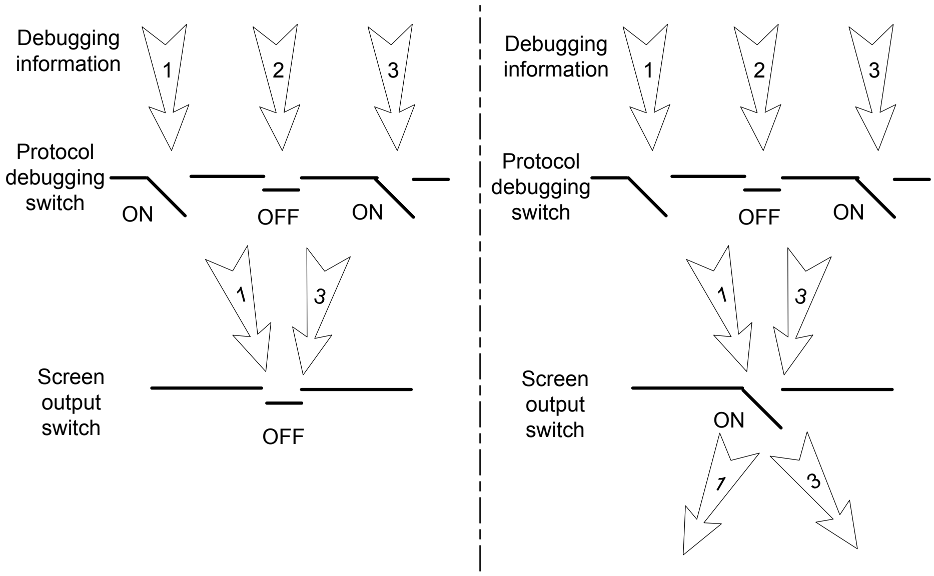
The device provides various debugging functions. For the majority of protocols and features supported, the system provides corresponding debugging information to help users diagnose errors.

The following two switches control the display of debugging information:

- Protocol debugging switch, which controls protocol-specific debugging information
- Screen output switch, which controls whether to display the debugging information on a certain screen.

Figure 2-1 illustrates the relationship between the protocol debugging switch and the screen output switch. Assume that the device can output debugging information to module 1, 2 and 3. Only when both are turned on can debugging information be output on a terminal.

Figure 2-1 The relationship between the protocol and screen debugging switch



Note

Displaying debugging information on the terminal is the most commonly used way to output debugging information. You can also output debugging information to other directions. For details, refer to *Information Center Operation*.

You can use the following commands to enable the two switches.

Follow these steps to enable debugging and terminal display for a specific module:

To do…	Use the command…	Remarks
Enable system debugging for specific module	**debugging** *module-name* [*debugging-option*]	Required Disabled for all modules by default.
Enable terminal display for debugging	**terminal debugging**	Required Disabled by default.

Caution

The output of debugging information affects the system operation. Disable all debugging after you finish the system debugging.

Displaying Debugging Status

To do…	Use the command…	Remarks
Display all enabled debugging on the specified device	**display debugging** [**fabric** | **unit** *unit-id*] [**interface** *interface-type interface-number*] [*module-name*]	Available in any view.
Display all enabled debugging in the Fabric by module	**display debugging fabric by-module**	

Displaying Operating Information about Modules in System

When an Ethernet switch is in trouble, you may need to view a lot of operating information to locate the problem. Each functional module has its corresponding operating information display command(s). You can use the command here to display the current operating information about the modules in the system for troubleshooting your system.

To do…	Use the command…	Remarks
Display the current operation information about the modules in the system.	**display diagnostic-information**	You can use this command in any view. You should execute this command twice to find the difference between the two executing results, thus helping locate the problem.

3 Network Connectivity Test

When configuring network connectivity test, go to these sections for information you are interested in:

- ping
- tracert

Network Connectivity Test

ping

You can use the **ping** command to check the network connectivity and the reachability of a host.

To do…	Use the command…	Remarks
Check the IP network connectivity and the reachability of a host	**ping** [**-a** *ip-address*] [**-c** *count*] [**-d**] [**-f**] [**-h** *ttl*] [**-i** *interface-type interface-number*] [**ip**] [**-n**] [**- p** *pattern*] [**-q**] [**-s** *packetsize*] [**-t** *timeout*] [**-tos** *tos*] [**-v**] *host*	You can execute this command in any view.

This command can output the following results:

- Response status for each ping packet. If no response packet is received within the timeout time, the message "Request time out" is displayed. Otherwise, the number of data bytes, packet serial number, time to live (TTL) and response time of the response packet are displayed.
- Final statistics, including the numbers of sent packets and received response packets, the irresponsive packet percentage, and the minimum, average and maximum values of response time.

tracert

You can use the **tracert** command to trace the gateways that a packet passes from the source to the destination. This command is mainly used to check the network connectivity. It can also be used to help locate the network faults.

The executing procedure of the **tracert** command is as follows: First, the source host sends a data packet with the TTL of 1, and the first hop device returns an ICMP error message indicating that it cannot forward this packet because of TTL timeout. Then, the source host resends the packet with the TTL of 2, and the second hop device also returns an ICMP TTL timeout message. This procedure goes on and on until the packet gets to the destination. During the procedure, the system records the source address of each ICMP TTL timeout message in order to offer the path that the packet passed through to the destination.

To do…	Use the command…	Remarks
View the gateways that a packet passes from the source host to the destination	**tracert** [**-a** *source-ip*] [**-f** *first-ttl*] [**-m** *max-ttl*] [**-p** *port*] [**-q** *num-packet*] [**-w** *timeout*] *string*	You can execute the **tracert** command in any view.

4 Device Management

When configuring device management, go to these sections for information you are interested in:

- Introduction to Device Management
- Device Management Configuration
- Displaying the Device Management Configuration
- Remote Switch APP Upgrade Configuration Example

Introduction to Device Management

Device Management includes the following:

- Reboot the Ethernet switch
- Configure real-time monitoring of the running status of the system
- Specify the APP to be used at the next reboot
- Update the Boot ROM
- Update the host software of the switches in the Fabric
- Identifying and Diagnosing Pluggable Transceivers

Device Management Configuration

Device Management Configuration Task list

Complete the following tasks to configure device management:

Task	Remarks
Rebooting the Ethernet Switch	Optional
Scheduling a Reboot on the Switch	Optional
Configuring Real-time Monitoring of the Running Status of the System	Optional
Specifying the APP to be Used at Reboot	Optional
Upgrading the Boot ROM	Optional
Upgrading the Host Software in the Fabric	Optional
Identifying and Diagnosing Pluggable Transceivers	Optional

Rebooting the Ethernet Switch

You can perform the following operation in user view when the switch is faulty or needs to be rebooted.

Note

Before rebooting, the system checks whether there is any configuration change. If yes, it prompts whether or not to proceed. This prevents the system from losing the configurations in case of shutting down the system without saving the configurations

Use the following command to reboot the Ethernet switch:

To do…	Use the command…	Remarks
Reboot the Ethernet switch	**reboot** [**unit** *unit-id*]	Available in user view

Scheduling a Reboot on the Switch

After you schedule a reboot on the switch, the switch will reboot at the specified time.

Follow these steps to schedule a reboot on the switch:

To do…	Use the command…	Remarks
Schedule a reboot on the switch, and set the reboot date and time	**schedule reboot at** *hh:mm* [*mm/dd/yyyy* | *yyyy/mm/dd*]	Optional
Schedule a reboot on the switch, and set the delay time for reboot	**schedule reboot delay** { *hh:mm* | *mm* }	Optional
Enter system view	**system-view**	—
Schedule a reboot on the switch, and set the reboot period	**schedule reboot regularity at** *hh:mm period*	Optional

Note

The switch timer can be set to precision of one minute, that is, the switch will reboot within one minute after the specified reboot date and time.

Configuring Real-time Monitoring of the Running Status of the System

This function enables you to dynamically record the system running status, such as CPU, thus facilitating analysis and solution of the problems of the device.

Follow these steps to configure real-time monitoring of the running status of the system:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable real-time monitoring of the running status of the system	**system-monitor enable**	Optional Enabled by default.

Caution

Enabling of this function consumes some amounts of CPU resources. Therefore, if your network has a high CPU usage requirement, you can disable this function to release your CPU resources.

Specifying the APP to be Used at Reboot

APP is the host software of the switch. If multiple APPs exist in the Flash memory, you can use the command here to specify the one that will be used when the switch reboots.

Use the following command to specify the APP to be used at reboot:

To do…	Use the command…	Remarks
Specify the APP to be used at reboot	**boot boot-loader** [**backup-attribute**] { *file-url* [**fabric**] | *device-name* }	Required

Upgrading the Boot ROM

You can use the Boot ROM program saved in the Flash memory of the switch to upgrade the running Boot ROM. With this command, a remote user can conveniently upgrade the Boot ROM by uploading the Boot ROM to the switch through FTP and running this command. The Boot ROM can be used when the switch restarts.

Use the following command to upgrade the Boot ROM:

To do…	Use the command…	Remarks
Upgrade the Boot ROM	**boot bootrom** { *file-url* | *device-name* }	Required

Upgrading the Host Software in the Fabric

You can execute the following command on any device in a Fabric to use specified host software to upgrade all devices in a Fabric, thus realizing the software version consistency in this Fabric.

To do…	Use the command…	Remarks
Upgrade the host software on the devices in the Fabric	**update fabric** { *file-url* | *device-name* }	Required

Identifying and Diagnosing Pluggable Transceivers

Introduction to pluggable transceivers

At present, four types of pluggable transceivers are commonly used, and they can be divided into optical transceivers and electrical transceivers based on transmission media as shown in Table 4-1.

Table 4-1 Commonly used pluggable transceivers

Transceiver type	Applied environment	Whether can be an optical transceiver	Whether can be an electrical transceiver
SFP (Small Form-factor Pluggable)	Generally used for 100M/1000M Ethernet interfaces or POS 155M/622M/2.5G interfaces	Yes	Yes
GBIC (GigaBit Interface Converter)	Generally used for 1000M Ethernet interfaces	Yes	Yes
XFP (10-Gigabit small Form-factor Pluggable)	Generally used for 10G Ethernet interfaces	Yes	No
XENPAK (10 Gigabit EtherNet Transceiver Package)	Generally used for 10G Ethernet interfaces	Yes	Yes

Identifying pluggable transceivers

As pluggable transceivers are of various types and from different vendors, you can perform the following configurations to identify main parameters of the pluggable transceivers, including transceiver type, connector type, central wavelength of the laser sent, transfer distance and vendor name or vendor name specified.

Follow these steps to identify pluggable transceivers:

To do…	Use the command…	Remarks
Display main parameters of the pluggable transceiver(s)	**display transceiver interface** [*interface-type* *interface-number*]	Available for all pluggable transceivers
Display part of the electrical label information of the anti-spoofing transceiver(s) customized by H3C	**display transceiver manuinfo interface** [*interface-type* *interface-number*]	Available for anti-spoofing pluggable transceiver(s) customized by H3C only

- You can use the **Vendor Name** field in the prompt information of the **display transceiver interface** command to identify an anti-spoofing pluggable transceiver customized by H3C. If the field is **H3C**, it is considered an H3C-customized pluggable transceiver.
- Electrical label information is also called permanent configuration data or archive information, which is written to the storage device of a card during device debugging or test. The information includes name of the card, device serial number, and vendor name or vendor name specified.

Diagnosing pluggable transceivers

The system outputs alarm information for you to diagnose and troubleshoot faults of pluggable transceivers. Optical transceivers customized by H3C also support the digital diagnosis function, which enables a transceiver to monitor the main parameters such as temperature, voltage, laser bias current, TX power, and RX power. When these parameters are abnormal, you can take corresponding measures to prevent transceiver faults.

Follow these steps to display pluggable transceiver information:

To do…	Use the command…	Remarks
Display the current alarm information of the pluggable transceiver(s)	**display transceiver alarm interface** [*interface-type interface-number*]	Available for all pluggable transceivers
Display the currently measured value of the digital diagnosis parameters of the anti-spoofing optical transceiver(s) customized by H3C	**display transceiver diagnosis interface** [*interface-type interface-number*]	Available for anti-spoofing pluggable optical transceiver(s) customized by H3C only

Displaying the Device Management Configuration

To do…	Use the command…	Remarks
Display the APP to be adopted at next startup	**display boot-loader** [**unit** *unit-id*]	Available in any view.
Display the module type and operating status of each board	**display device** [**manuinfo** [**unit** *unit-id*] | **unit** *unit-id*]	
Display CPU usage of a switch	**display cpu** [**unit** *unit-id*]	
Display the operating status of the fan	**display fan** [**unit** *unit-id* [*fan-id*]]	
Display memory usage of a switch	**display memory** [**unit** *unit-id*]	
Display the operating status of the power supply	**display power** [**unit** *unit-id* [*power-id*]]	
Display system diagnostic information or save system diagnostic information to a file with the extension .diag into the Flash memory	**display diagnostic-information**	
Display enabled debugging on a specified switch or all switches in the fabric	**display debugging** { **fabric** | **unit** *unit-id* } [**interface** *interface-type interface-number*] [*module-name*]	
Display enabled debugging on all switches in the fabric by modules	**display debugging fabric by-module**	

Remote Switch APP Upgrade Configuration Example

Network requirements

Telnet to the switch from a PC remotely and download applications from the FTP server to the Flash memory of the switch. Update the switch software by using the device management commands through CLI.

The switch acts as the FTP client, and the remote PC serves as both the configuration PC and the FTP server.

Perform the following configuration on the FTP server.

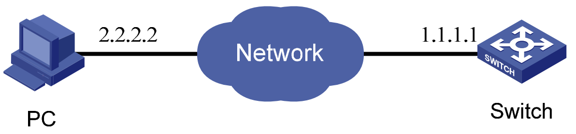
- Configure an FTP user, whose name is switch and password is **hello**. Authorize the user with the read-write right on the directory Switch on the PC.

- Make configuration so that the IP address of a VLAN interface on the switch is 1.1.1.1, the IP address of the PC is 2.2.2.2, and the switch and the PC is reachable to each other.

The host software switch.app and the Boot ROM file boot.btm of the switch are stored in the directory **switch** on the PC. Use FTP to download the switch.app and boot.btm files from the FTP server to the switch.

Network diagram

Figure 4-1 Network diagram for FTP configuration



Configuration procedure

1) Configure the following FTP server–related parameters on the PC: an FTP user with the username as switch and password as hello, who is authorized with the read-write right on the directory Switch on the PC. The detailed configuration is omitted here.
2) On the switch, configure a level 3 telnet user with the username as user and password as hello. Authentication mode is by user name and password.

Note

Refer to the *Login Operation* part of this manual for configuration commands and steps about telnet user.

---

3) Execute the **telnet** command on the PC to log into the switch. The following prompt appears:

```
<Sysname>
```

Caution

If the Flash memory of the switch is not sufficient, delete the original applications before downloading the new ones.

---

4) Initiate an FTP connection with the following command in user view. Enter the correct user name and password to log into the FTP server.

```
<Sysname> ftp 2.2.2.2
Trying ...
Press CTRL+K to abort
Connected.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(none):switch
```

```
331 Give me your password, please
Password:
230 Logged in successfully
[ftp]
```

5) Enter the authorized path on the FTP server.

```
[ftp] cd switch
```

6) Execute the **get** command to download the switch.app and boot.btm files on the FTP server to the Flash memory of the switch.

```
[ftp] get switch.app
[ftp] get boot.btm
```

7) Execute the **quit** command to terminate the FTP connection and return to user view.

```
[ftp] quit
<Sysname>
```

8) Upgrade the Boot ROM.

```
<Sysname> boot bootrom boot.btm
This will update BootRom file on unit 1. Continue? [Y/N] y
 Upgrading BOOTROM, please wait...
 Upgrade BOOTROM succeeded!
```

9) Specify the downloaded program as the host software to be adopted when the switch starts next time.

```
<Sysname> boot boot-loader switch.app
 The specified file will be booted next time on unit 1!
<Sysname> display boot-loader
 Unit 1:
   The current boot app is: switch.app
   The main boot app is:    switch.app
   The backup boot app is:
```

Reboot the switch to upgrade the Boot ROM and host software of the switch.

```
<Sysname> reboot
 Start to check configuration with next startup configuration file,
 please wait......
 This command will reboot the device. Current configuration may be lost in next startup if
you continue.   Continue? [Y/N] y
 This will reboot device. Continue? [Y/N] y
```

Table of Contents

1 VLAN-VPN Configuration

When configuring VLAN-VPN, go to these sections for information you are interested in:

- VLAN-VPN Overview
- VLAN-VPN Configuration
- Displaying and Maintaining VLAN-VPN Configuration
- VLAN-VPN Configuration Example

VLAN-VPN Overview

Introduction to VLAN-VPN

Virtual private network (VPN) is a new technology that emerges with the expansion of the Internet. It can be used for establishing private networks over the public network. With VPN, you can specify to process packets on the client or the access end of the service provider in specific ways, establish dedicated tunnels for user traffic on public network devices, and thus improve data security.

VLAN-VPN feature is a simple yet flexible Layer 2 tunneling technology. It tags private network packets with outer VLAN tags, thus enabling the packets to be transmitted through the service providers' backbone networks with both inner and outer VLAN tags. In public networks, packets of this type are transmitted by their outer VLAN tags (that is, the VLAN tags of public networks), and the inner VLAN tags are treated as part of the payload.

Figure 1-1 describes the structure of the packets with single-layer VLAN tags.

Figure 1-1 Structure of packets with single-layer VLAN tags

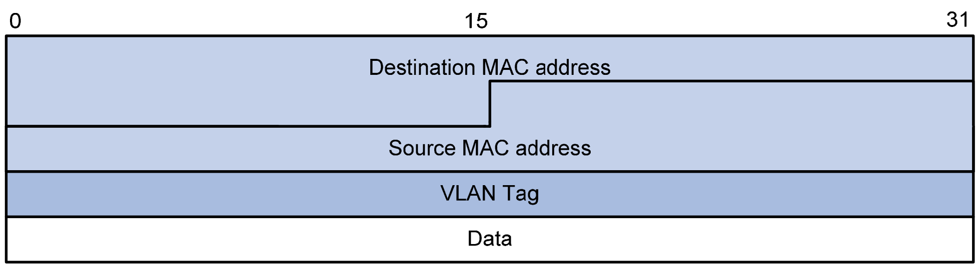
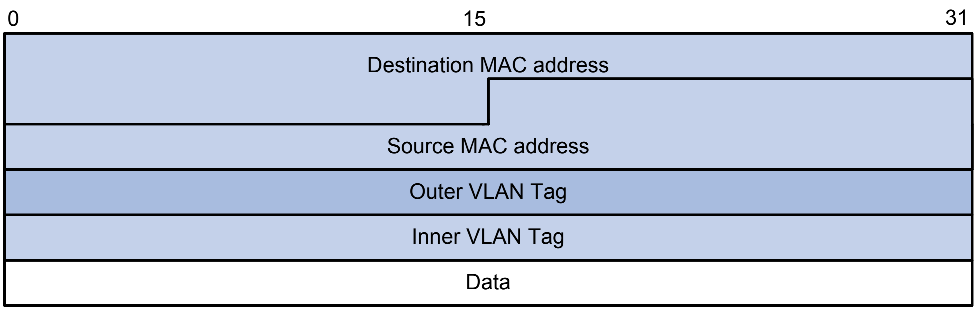


Figure 1-2 describes the structure of the packets with double-layer VLAN tags.

Figure 1-2 Structure of packets with double-layer VLAN tags



Compared with MPLS-based Layer 2 VPN, VLAN-VPN has the following features:

- It provides Layer 2 VPN tunnels that are simpler.
- VLAN-VPN can be implemented through manual configuration. That is, signaling protocol-related configuration is not needed.

The VLAN-VPN feature provides you with the following benefits:

- Saves public network VLAN ID resource.
- You can have VLAN IDs of your own, which is independent of public network VLAN IDs.
- Provides simple Layer 2 VPN solutions for small-sized MANs or intranets.

Implementation of VLAN-VPN

With the VLAN-VPN feature enabled, no matter whether or not a received packet already carries a VLAN tag, the switch will tag the received packet with the default VLAN tag of the receiving port and add the source MAC address to the MAC address table of the default VLAN. When a packet reaches a VLAN-VPN-enabled port:

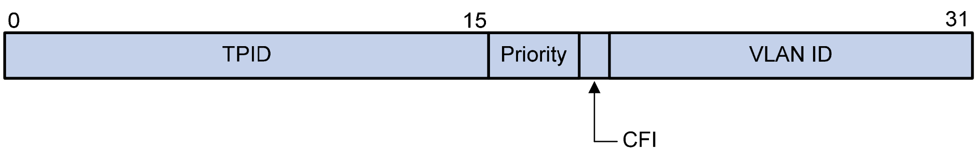
- If the packet already carries a VLAN tag, the packet becomes a dual-tagged packet.
- Otherwise, the packet becomes a packet carrying the default VLAN tag of the port.

Configuring the TPID for VLAN-VPN Packets

A VLAN tag uses the tag protocol identifier (TPID) field to identify the protocol type of the tag. The value of this field is 0x8100 for IEEE 802.1Q.

Figure 1-3 illustrates the structure of the IEEE 802.1Q VLAN tag in an Ethernet frame.

Figure 1-3 The structure of the VLAN tag in an Ethernet frame



A Switch 4500 switch determines whether a received frame is VLAN tagged by comparing its own TPID with the TPID field in the received frame. If they match, the frame is considered as a VLAN tagged frame. If not, the switch tags the frame with the default VLAN tag of the receiving port.

By default, Switch 4500 series switches adopt the IEEE 802.1Q TPID value 0x8100. Some vendors, however, use other TPID values such as 0x9100. For compatibility with these systems, the Switch 4500 series switches allow you to change the TPID that a port uses when tagging a received VLAN-VPN

frame as needed. When doing that, you should set the same TPID on both the customer-side port and the service provider-side port.

The TPID in an Ethernet frame has the same position with the protocol type field in a frame without a VLAN tag. To avoid problems in packet forwarding and handling, you cannot set the TPID value to any of the values in the table below.

Table 1-1 Commonly used protocol type values in Ethernet frames

Protocol type	Value
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1x	0x888E

Inner-to-Outer Tag Priority Replicating and Mapping

As shown in Figure 1-3, the user priority field is the 802.1p priority of the tag. The value of this 3-bit field is in the range 0 to 7. By configuring inner-to-outer tag priority replicating or mapping for a VLAN-VPN-enabled port, you can replicate the inner tag priority to the outer tag or assign outer tags of different priorities to packets according to their inner tag priorities.

Refer to *QoS* part for information about priority.

Transparent IGMP Message Transmission on a VLAN-VPN Port

Note

For detailed information about IGMP messages and how a switch processes IGMP messages of different types, refer to the *Multicast* module in this manual.

For a VLAN-VPN-disabled port, the switch transparently transmits an IGMP message received on the port within the VLAN that the IGMP message belongs to. For the switch to transparently transmit an IGMP message received on a VLAN-VPN port in the outer VLAN, you must enable transparent IGMP message transmission on the port.

VLAN-VPN Configuration

VLAN-VPN Configuration Task List

Complete the following tasks to configure VLAN-VPN:

Task	Remarks
Enabling the VLAN-VPN Feature for a Port	Required
Configuring the TPID Value for VLAN-VPN Packets on a Port	Optional
Configuring the Inner-to-Outer Tag Priority Replicating and Mapping Feature	Optional

Caution

As XRN fabric is mutually exclusive with VLAN-VPN, make sure that XRN fabric is disabled on the switch before performing any of the configurations listed in the above table. For information about XRN fabric, refer to *XRN Fabric Configuration* in this manual.

Enabling the VLAN-VPN Feature for a Port

Follow these steps to enable the VLAN-VPN feature for a port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the VLAN-VPN feature on the port	**vlan-vpn enable**	Required By default, the VLAN-VPN feature is disabled on a port.

Configuring the TPID Value for VLAN-VPN Packets on a Port

For your device to correctly identify the VLAN tagged frames from the public network, make sure that the TPID you will use is the same as that used on the peer device in the public network.

Follow these steps to configure the TPID for VLAN-VPN packets on a port:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Set the TPID value on the port	**vlan-vpn tpid** *value*	Required Do not set the TPID value to any of the protocol type values listed in Table 1-1. For 3Com series switches, the TPID defaults to 0x8100.

Note

- Besides the default TPID 0x8100, you can configure only one TPID value on a Switch 4500 switch.
- For the Switch 4500 series to exchange packets with the public network device properly, you should configure the TPID value used by the public network device on both the customer-side port and the service provider-side port.

Configuring the Inner-to-Outer Tag Priority Replicating and Mapping Feature

Make sure that the VLAN-VPN feature is enabled on a port before configuring the inner-to-outer tag priority replicating and mapping feature.

Follow these steps to configure the inner-to-outer tag priority replicating and mapping feature:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Enable the inner-to-outer tag priority replicating feature	**vlan-vpn inner-cos-trust enable**	Either of the two configurations is required. By default, neither the inner-to-outer tag priority replicating feature nor the inner-to-outer tag priority mapping feature is enabled.
Enable the inner-to-outer tag priority mapping feature and create a priority mapping	**vlan-vpn priority** *old-priority* **remark** *new-priority*	

Caution

- If you have configured the port priority (refer to *QoS Configuration* part in this manual), you will be prompted that the port priority configured for the current port gets invalid after you enable the inner-to-outer tag priority replicating feature.
- The inner-to-outer tag priority replicating feature is mutually exclusive with the inner-to-outer tag priority mapping feature.

Displaying and Maintaining VLAN-VPN Configuration

To do...	Use the command...	Remarks
Display the VLAN-VPN configurations of all the ports	**display port vlan-vpn**	Available in any view

VLAN-VPN Configuration Example

Transmitting User Packets through a Tunnel in the Public Network by Using VLAN-VPN

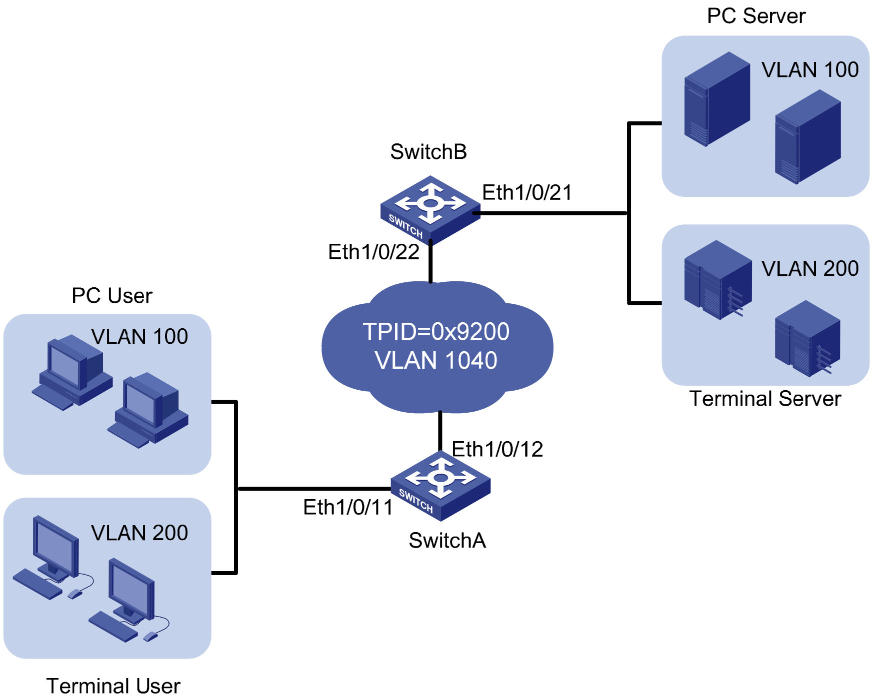
Network requirements

As shown in Figure 1-4, Switch A and Switch B are both Switch 4500 series switches. They connect the users to the servers through the public network.

- PC users and PC servers are in VLAN 100 created in the private network, while terminal users and terminal servers are in VLAN 200, which is also created in the private network. The VLAN VPN connection is established in VLAN 1040 of the public network.
- Switches of other vendors' are used in the public network. They use the TPID value 0x9200.
- Employ VLAN-VPN on Switch A and Switch B to enable the PC users and PC servers to communicate with each through a VPN, and employ VLAN-VPN on Switch A and Switch B to enable the Terminal users and Terminal servers to communicate with each other through a VPN.

Network diagram

Figure 1-4 Network diagram for VLAN-VPN configuration



Configuration procedure

- Configure Switch A.

Enable the VLAN-VPN feature on Ethernet 1/0/11 of Switch A and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.

```
<SwitchA> system-view
[SwitchA] vlan 1040
[SwitchA-vlan1040] port Ethernet 1/0/11
[SwitchA-vlan1040] quit
[SwitchA] interface Ethernet 1/0/11
```

```
[SwitchA-Ethernet1/0/11] vlan-vpn enable
[SwitchA-Ethernet1/0/11] quit
```

Set the TPID value of Ethernet 1/0/12 to 0x9200 (for intercommunication with the devices in the public network) and configure the port as a trunk port permitting packets of VLAN 1040.

```
[SwitchA] interface Ethernet 1/0/12
[SwitchA-Ethernet1/0/12] vlan-vpn tpid 9200
[SwitchA-Ethernet1/0/12] port link-type trunk
[SwitchA-Ethernet1/0/12] port trunk permit vlan 1040
```

- Configure Switch B.

Enable the VLAN-VPN feature on Ethernet 1/0/21 of Switch B and tag the packets received on this port with the tag of VLAN 1040 as the outer VLAN tag.

```
<SwitchB> system-view
[SwitchB] vlan 1040
[SwitchB-vlan1040] port Ethernet 1/0/21
[SwitchB-vlan1040] quit
[SwitchB] interface Ethernet 1/0/21
[SwitchB-Ethernet1/0/21] vlan-vpn enable
```

Set the TPID value of Ethernet1/0/22 to 0x9200 (for intercommunication with the devices in the public network) and set the port as a trunk port permitting packets of VLAN 1040.

```
[SwitchB-Ethernet1/0/22] vlan-vpn tpid 9200
[SwitchB-Ethernet1/0/22] quit
[SwitchB] interface Ethernet 1/0/21
[SwitchB-Ethernet1/0/22] port link-type trunk
[SwitchB-Ethernet1/0/22] port trunk permit vlan 1040
```

Note

- Do not configure VLAN 1040 as the default VLAN of Ethernet 1/0/12 of Switch A and Ethernet 1/0/22 of Switch B. Otherwise, the outer VLAN tag of a packet will be removed during transmission.
- In this example, both Ethernet1/0/11 of Switch A and Ethernet1/0/21 of Switch B are access ports. In cases where the ports are trunk ports or hybrid ports, you need to configure the two ports to remove the outer VLAN tags before transmitting packets of VLAN 1040. Refer to *VLAN* in this manual for detailed configuration.

- Configure the devices in the public network

As the devices in the public network are from other vendors, only the basic principles are introduced here. That is, you need to configure the devices connecting to Ethernet 1/0/12 of Switch A and Ethernet 1/0/22 of Switch B to permit the corresponding ports to transmit tagged packets of VLAN 1040.

Data transfer process

The following describes how a packet is forwarded from Switch A to Switch B in this example.

1) As Ethernet 1/0/11 of Switch A is a VLAN-VPN port, when a packet from the customer's network side reaches this port, it is tagged with the default VLAN tag of the port (VLAN 1040).

2) The TPID value of the outer VLAN tag is set to 0x9200 before the packet is forwarded to the public network through Ethernet1/0/12 of Switch A.
3) The outer VLAN tag of the packet remains unchanged while the packet travels in the public network, till it reaches Ethernet1/0/22 of Switch B.
4) After the packet reaches Switch B, it is forwarded through Ethernet1/0/21 of Switch B. As the port belongs to VLAN 1040 and is an access port, the outer VLAN tag (the tag of VLAN 1040) of the packet is removed before the packet is forwarded, which restores the packet to a packet tagged with only the private VLAN tag and enables it to be forwarded to its destination networks.
5) It is the same case when a packet travels from Switch B to Switch A.

2 Selective QinQ Configuration

When configuring selective QinQ, go to these sections for information you are interested in:

- Selective QinQ Overview
- Selective QinQ Configuration
- Selective QinQ Configuration Example

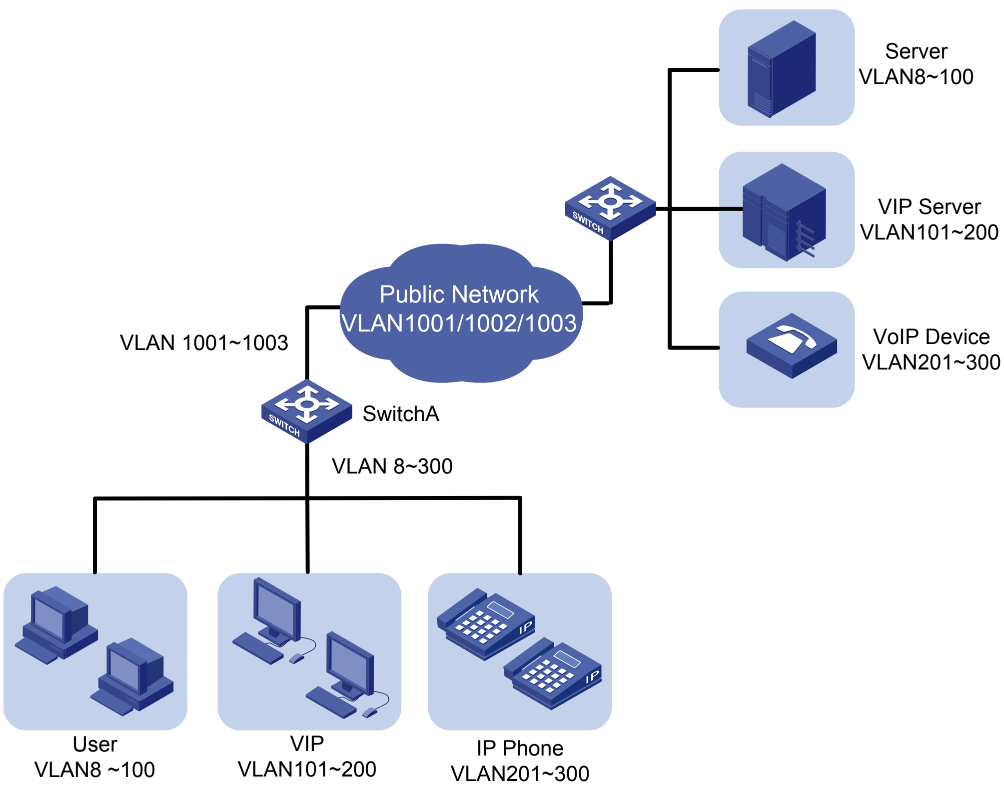
Selective QinQ Overview

Selective QinQ Overview

Selective QinQ is an enhanced application of the VLAN-VPN feature. With the selective QinQ feature, you can configure inner-to-outer VLAN tag mapping, according to which you can add different outer VLAN tags to the packets with different inner VLAN tags.

The selective QinQ feature makes the service provider network structure more flexible. You can classify the terminal users on the port connecting to the access layer device according to their VLAN tags, and add different outer VLAN tags to these users. In the public network, you can configure QoS policies based on outer VLAN tags to assign different priorities to different packets, thus providing differentiated services. See Figure 2-1 for details.

Figure 2-1 Diagram for a selective QinQ implementation



In this implementation, Switch A is an access device of the service provider. The users connecting to it include common customers (in VLAN 8 to VLAN 100), VIPs (in VLAN 101 to VLAN 200), and IP

telephone users (in VLAN 201 to VLAN 300). Packets of all these users are forwarded by Switch A to the public network.

After the selective QinQ feature and the inner-to-outer tag mapping feature are enabled on the port connecting Switch A to these users, the port will add different outer VLAN tags to the packets according to their inner VLAN tags. For example, you can configure to add the tag of VLAN 1002 to the packets of IP telephone users in VLAN 201 to VLAN 300 and forward the packets to the VoIP device, which is responsible for processing IP telephone services.

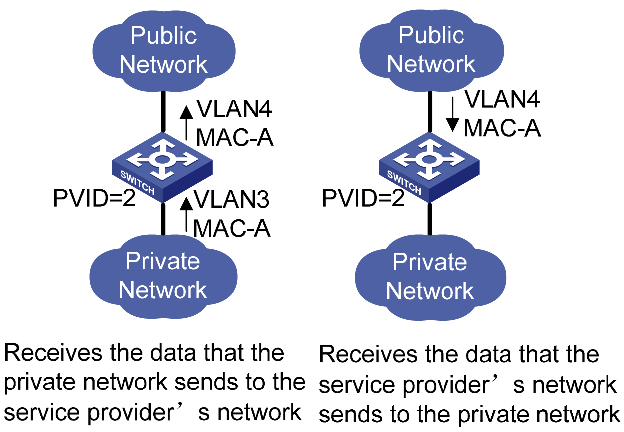
To guarantee the quality of voice packet transmission, you can configure QoS policies in the public network to reserve bandwidth for packets of VLAN 1002 and forward them preferentially.

In this way, you can configure different forwarding policies for data of different type of users, thus improving the flexibility of network management. On the other hand, network resources are well utilized, and users of the same type are also isolated by their inner VLAN tags. This helps to improve network security.

MAC Address Replicating

Like the VLAN-VPN feature, a port with the selective QinQ enabled adds the source MAC addresses of user packets to the MAC address table of the default VLAN on the port. However, the port with selective QinQ enabled can insert an outer VLAN tag other than that of the default VLAN to the packets. Thus, when packets are forwarded from the service provider to users, they may be broadcast if their destination MAC addresses cannot be found in the MAC address table of the outer VLANs.

Figure 2-2 Learn MAC addresses of selective QinQ packets



As shown in Figure 2-2, the default VLAN of the port used to receive packets is VLAN 2. The port is configured to receive packets of VLAN 3, tag the received packets with the outer tag of VLAN 4, and add the source MAC addresses (MAC-A) of the packets to the MAC address table of its default VLAN (VLAN 2).

When a response packet is returned to the device from VLAN 4 of the service provider network, the device searches the outbound port for MAC-A in the MAC address table of VLAN 4. However, because the corresponding entry is not added to the MAC address table of VLAN 4, this packet is considered to be a unicast packet with unknown destination MAC address. As a result, this packet will be broadcast to all the ports in VLAN 4, which wastes the network resources and incurs potential security risks.

The Switch 4500 series Ethernet switches provide the inter-VLAN MAC address replicating feature, which can replicate the entries in the MAC address table of the default VLAN to that of the VLAN corresponding to the outer tag. With the inter-VLAN MAC address replicating feature enabled, when a

device receives a packet from the service provider network, this device will find the path for the packet by searching the MAC address table of the VLAN corresponding to the outer tag and unicast the packet. Thus, packet broadcast is reduced in selective QinQ applications.

Likewise, the entries in the MAC address table of the outer VLAN can also be replicated to that of the default VLAN on a port, through which the outbound port to the service provider network can be determined through the MAC address table of the default VLAN and user packets destined for the service provider can be unicast.

Selective QinQ Configuration

Selective QinQ Configuration Task List

Complete the following tasks to configure selective QinQ:

Task	Remarks
Enabling the Selective QinQ Feature for a Port	Required
Enabling the Inter-VLAN MAC Address Replicating Feature	Optional

Caution

If XRN Fabric has been enabled on a device, you cannot enable the VLAN-VPN feature and the selective QinQ feature on any port of the device.

Enabling the Selective QinQ Feature for a Port

The following configurations are required for the selective QinQ feature:

- Enabling the VLAN-VPN feature on the current port
- Configuring the current port to permit packets of specific VLANs (the VLANs whose tags are to be used as the outer VLAN tags are required)

Follow these steps to enable the selective QinQ feature:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the outer VLAN tag and enter QinQ view	**vlan-vpn vid** *vlan-id*	Required
Configure to add outer VLAN tags to the packets with the specific inner VLAN tags	**raw-vlan-id inbound** *vlan-id-list*	Required By default, the feature of adding an outer VLAN tag to the packets with the specific inner VLAN tags is disabled.

Note

Do not enable both the selective QinQ function and the DHCP snooping function on a switch. Otherwise, the DHCP snooping function may operate improperly.

Enabling the Inter-VLAN MAC Address Replicating Feature

Follow these steps to enable the inter-VLAN MAC address replicating feature:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Enable the inter-VLAN MAC address replicating feature	**mac-address-mapping** *index* **source-vlan** *source-vlan-id-list* **destination-vlan** *dest-vlan-id*	Required By default, the inter-VLAN MAC address replicating feature is disabled.

Caution

- On a port, the inter-VLAN MAC address replicating feature can be configured only once for a destination VLAN. If the configuration needs to be modified, you need to remove the existing configuration first.
- With the inter-VLAN MAC address replicating feature disabled, all the MAC address entries that the destination VLAN learns from the other VLANs through this function are removed.
- MAC address entries obtained through the inter-VLAN MAC address replicating feature cannot be removed manually. To remove a MAC address entry of this kind, you need to disable the inter-VLAN MAC address replicating feature first.
- VLAN 4093 is a special VLAN reserved for the XRN fabric feature. It can not serve as the destination VLAN of the inter-VLAN MAC address replicating feature to receive MAC address entries from the other VLANs.

Selective QinQ Configuration Example

Processing Private Network Packets by Their Types

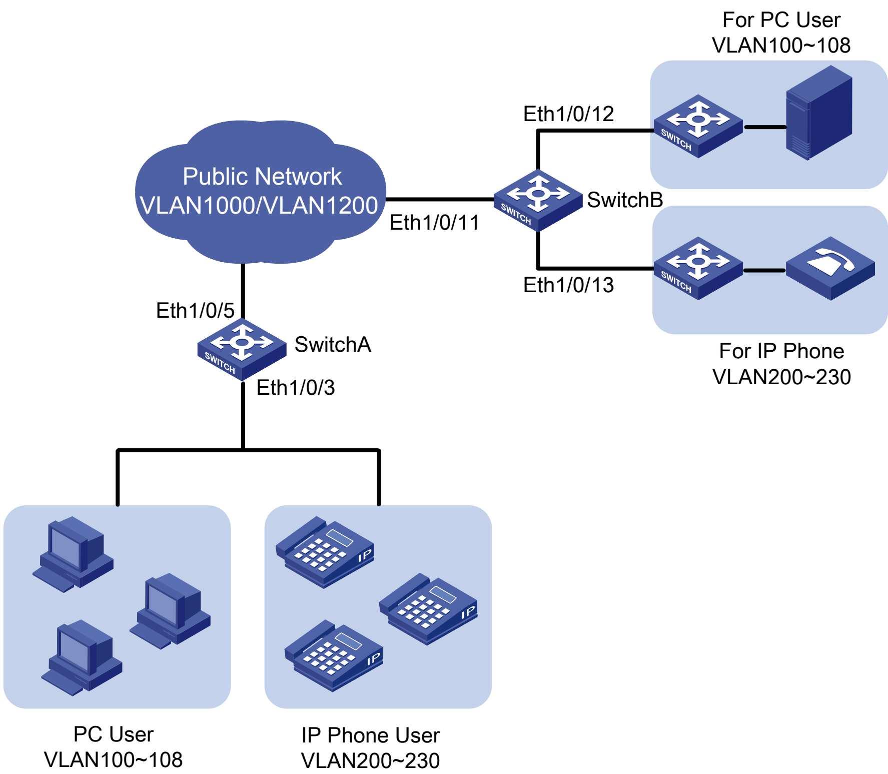
Network requirements

- Ethernet 1/0/3 of Switch A provides public network access for PC users and IP phone users. PC users belong to VLAN 100 through VLAN 108, and IP phone users belong to VLAN 200 through VLAN 230. Ethernet 1/0/5 of Switch A is connected to the public network. The peer end of Switch A is Switch B.
- Ethernet 1/0/11 of Switch B is connected to the public network. Ethernet 1/0/12 and Ethernet1/0/13 of Switch B provide network access for PC servers belonging to VLAN 100 through VLAN 108 and voice gateways (for IP phone users) belonging to VLAN 200 through VLAN 230 respectively.

- The public network permits packets of VLAN 1000 and VLAN 1200. Apply QoS policies for these packets to reserve bandwidth for packets of VLAN 1200. That is, packets of VLAN 1200 have higher transmission priority over packets of VLAN 1000.
- Employ the selective QinQ feature on Switch A and Switch B to differentiate traffic of PC users from that of IP phone users, for the purpose of using QoS policies to guarantee higher priority for voice traffic.
- To reduce broadcast packets in the network, enable the inter-VLAN MAC address replicating feature for selective QinQ.

Network diagram

Figure 2-3 Network diagram for selective QinQ configuration



Configuration procedure

- Configure Switch A.

Create VLAN 1000, VLAN 1200 and VLAN 5 (the default VLAN of Ethernet 1/0/3) on SwitchA.

```
<SwitchA> system-view
[SwitchA] vlan 1000
[SwitchA-vlan1000] quit
[SwitchA] vlan 1200
[SwitchA-vlan1200] quit
[SwitchA] vlan 5
[SwitchA-vlan5] quit
```

Configure Ethernet 1/0/5 as a hybrid port and configure it not to remove VLAN tags when forwarding packets of VLAN 5, VLAN 1000, and VLAN 1200.

```
[SwitchA] interface Ethernet 1/0/5
[SwitchA-Ethernet1/0/5] port link-type hybrid
```

```
[SwitchA-Ethernet1/0/5] port hybrid vlan 5 1000 1200 tagged
[SwitchA-Ethernet1/0/5] quit
```

Configure Ethernet 1/0/3 as a hybrid port and configure VLAN 5 as its default VLAN. Configure Ethernet 1/0/3 to remove VLAN tags when forwarding packets of VLAN 5, VLAN 1000, and VLAN 1200.

```
[SwitchA] interface Ethernet 1/0/3
[SwitchA-Ethernet1/0/3] port link-type hybrid
[SwitchA-Ethernet1/0/3] port hybrid pvid vlan 5
[SwitchA-Ethernet1/0/3] port hybrid vlan 5 1000 1200 untagged
```

Enable the VLAN-VPN feature on Ethernet 1/0/3.

```
[SwitchA-Ethernet1/0/3] vlan-vpn enable
```

Enable the selective QinQ feature on Ethernet 1/0/3 to tag packets of VLAN 100 through VLAN 108 with the tag of VLAN 1000 as the outer VLAN tag, and tag packets of VLAN 200 through VLAN 230 with the tag of VLAN 1200 as the outer VLAN tag.

```
[SwitchA-Ethernet1/0/3] vlan-vpn vid 1000
[SwitchA-Ethernet1/0/3-vid-1000] raw-vlan-id inbound 100 to 108
[SwitchA-Ethernet1/0/3-vid-1000] quit
[SwitchA-Ethernet1/0/3] vlan-vpn vid 1200
[SwitchA-Ethernet1/0/3-vid-1200] raw-vlan-id inbound 200 to 230
```

Enable the inter-VLAN MAC address replicating feature to replicate the MAC address entries of the MAC address tables of the outer VLANs to the MAC address table of the default VLAN, and replicate the MAC address entries of the MAC address table of the default VLAN to the MAC address tables of the outer VLANs.

```
[SwitchA-Ethernet1/0/3-vid-1200] quit
[SwitchA-Ethernet1/0/3] mac-address mapping 0 source-vlan 5 destination-vlan 1000
[SwitchA-Ethernet1/0/3] mac-address mapping 1 source-vlan 5 destination-vlan 1200
[SwitchA-Ethernet1/0/3] quit
[SwitchA] interface Ethernet 1/0/5
[SwitchA-Ethernet1/0/5] mac-address mapping 0 source-vlan 1000 1200 destination-vlan 5
```

After the above configuration, packets of VLAN 100 through VLAN 108 (that is, packets of PC users) are tagged with the tag of VLAN 1000 as the outer VLAN tag when they are forwarded to the public network by Switch A; and packets of VLAN 200 through VLAN 230 (that is, packets of IP phone users) are tagged with the tag of VLAN 1200 as the outer VLAN tag when they are forwarded to the public network.

- Configure Switch B.

Create VLAN 1000, VLAN 1200, VLAN 12 (the default VLAN of Ethernet1/0/12) and VLAN 13 (the default VLAN of Ethernet1/0/13) on Switch B.

```
<SwitchB> system-view
[SwitchB] vlan 1000
[SwitchB-vlan1000] quit
[SwitchB] vlan 1200
[SwitchB-vlan1200] quit
[SwitchB] vlan 12 to 13
```

Configure Ethernet 1/0/11 as a hybrid port, and configure Ethernet 1/0/11 not to remove VLAN tags when forwarding packets of VLAN 12, VLAN 13, VLAN 1000, and VLAN 1200.

```
<SwitchB> system-view
```

```
[SwitchB] interface Ethernet 1/0/11
[SwitchB-Ethernet1/0/11] port link-type hybrid
[SwitchB-Ethernet1/0/11] port hybrid vlan 12 13 1000 1200 tagged
```

Configure Ethernet1/0/12 as a hybrid port and configure VLAN 12 as its default VLAN . Configure Ethernet 1/0/12 to remove VLAN tags when forwarding packets of VLAN 12 and VLAN 1000.

```
[SwitchB] interface Ethernet 1/0/12
[SwitchB-Ethernet1/0/12] port link-type hybrid
[SwitchB-Ethernet1/0/12] port hybrid pvid  vlan 12
[SwitchB-Ethernet1/0/12] port hybrid vlan 12 1000 untagged
[SwitchB-Ethernet1/0/12] quit
```

Configure Ethernet 1/0/13 as a hybrid port and configure VLAN 13 as its default VLAN . Configure Ethernet 1/0/13 to remove VLAN tags when forwarding packets of VLAN 13 and VLAN 1200.

```
[SwitchB] interface Ethernet 1/0/13
[SwitchB-Ethernet1/0/13] port link-type hybrid
[SwitchB-Ethernet1/0/13] port hybrid pvid vlan 13
[SwitchB-Ethernet1/0/13] port hybrid vlan 13 1200 untagged
```

After the above configuration, Switch B can forward packets of VLAN 1000 and VLAN 1200 to the corresponding servers through Ethernet 1/0/12 and Ethernet 1/0/13 respectively.

To make the packets from the servers be transmitted to the clients in the same way, you need to configure the selective QinQ feature and the inter-VLAN MAC address replicating feature on Ethernet 1/0/12 and Ethernet 1/0/13. The configuration on Switch B is similar to that on Switch A and is thus omitted.

Note

- The port configuration on Switch B is only an example for a specific network requirement. The key to this example is to enable the ports to receive and forward packets of specific VLANs. So you can also configure the ports as trunk ports. Refer to *VLAN Configuration* for details.
- A selective QinQ-enabled device tags a user packet with an outer VLAN tag regardless of the VLAN tag of the user packet, so there is no need to configure user VLANs on the device.
- Make sure the packets of the default VLAN of a selective QinQ-enabled port are permitted on both the local port and the port connecting to the public network.

Table of Contents

1 Remote-ping Configuration

Introduction to remote-ping

remote-ping is a network diagnostic tool used to test the performance of protocols (only ICMP by far) running on network. It is an enhanced alternative to the **ping** command.

remote-ping test group is a set of remote-ping test parameters. A test group contains several test parameters and is uniquely identified by an administrator name plus a test tag.

You can perform an remote-ping test after creating a test group and configuring the test parameters.

Different from the **ping** command, remote-ping does not display the round trip time (RTT) and timeout status of each packet on the console terminal in real time. You need to execute the **display remote-ping** command to view the statistic results of your remote-ping test operation. remote-ping allows setting the parameters of remote-ping test groups and starting remote-ping test operations through network management system.

Figure 1-1 Illustration for remote-ping

remote-ping Configuration

Introduction to remote-ping Configuration

The configuration tasks for remote-ping include:

- Enabling remote-ping Client
- Creating test group
- Configuring test parameters

The test parameters that you can configure include:

1) Destination IP address

It is equivalent to the destination IP address in the **ping** command.

2) Test type

Currently, remote-ping supports only one test type: ICMP.

3) Number of test packets to be sent in a test

If this parameter is set to a number greater than 1, the system sends the second test packet once it receives a response to the first one, or when the test timer times out if it receives no response after sending the first one, and so forth until the last test packet is sent out. This parameter is equivalent to the **–n** keyword in the **ping** command.

4) Automatic test interval

This parameter is used to enable the system to automatically perform the same test at regular intervals.

5) Test timeout time

Test timeout time is the duration while the system waits for an ECHO-RESPONSE packet after it sends out an ECHO-REQUEST packet. If no ECHO-RESPONSE packet is received within this duration, this test is considered a failure. This parameter is similar to the **-t** keyword in the **ping** command, but has a different unit (the **-t** keyword in the **ping** command is in milliseconds, while the timeout time in the **remote-ping** command is in seconds).

Configuring remote-ping

Table 1-1 Configure remote-ping

Operation	Command	Description
Enter system view	**system-view**	—
Enable remote-ping Client	**remote-ping-agent enable**	Required By default, remote-ping Client is disabled.
Create an remote-ping test group	**remote-ping** *administrator-name operation-tag*	Required By default, no remote-ping test group is configured.
Configure the destination IP address of the test	**destination-ip** *ip-address*	Required By default, no destination IP address is configured.
Configure the test type	**test-type** *type*	Optional By default, the test type is ICMP.
Configure the number of packets to be sent in each test.	**count** *times*	Optional By default, the number of packets to be sent in each test is 1.
Configure the automatic test interval.	**frequency** *interval*	Optional By default, the automatic test interval is zero, indicating no automatic test will be performed.
Configure the timeout time of the test.	**timeout** *time*	Optional By default, the timeout time is 3 seconds.
Execute the test	**test-enable**	Required

Displaying remote-ping Configuration

After the above remote-ping configuration, you can execute the **display** command in any view to display the information of remote-ping test operation status to you can verify the configuration effect.

Table 1-2 Display remote-ping configuration

Operation	Command	Description
Display the information of remote-ping test history	**display remote-ping history** [*administrator-name operation-tag*]	The **display** command can be executed in any view.
Display the latest remote-ping test results	**display remote-ping results** [*administrator-name operation-tag*]	

Configuration Example

Network requirement

Perform an remote-ping ICMP test between two switches. Like a ping test, this test uses ICMP to test the RTTs of data packets between the source and the destination.

Configuration procedure

Enable remote-ping Client.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] remote-ping-agent enable
```

Create an remote-ping test group “administrator icmp”.

```
[Sysname] remote-ping administrator icmp
```

Specify the test type as ICMP.

```
[Sysname-remote-ping-administrator-icmp] test-type icmp
```

Specify the destination IP address as 1.1.1.99.

```
[Sysname-remote-ping-administrator-icmp] destination-ip 1.1.1.99
```

Set the number of test packets sent in a test to 10.

```
[Sysname-remote-ping-administrator-icmp] count 10
```

Set the timeout time of test operations to 5.

```
[Sysname-remote-ping-administrator-icmp] timeout 5
```

Enable the test operation.

```
[Sysname-remote-ping-administrator-icmp] test-enable
```

Display the test results.

```
[Sysname-remote-ping-administrator-icmp] display remote-ping results administrator icmp
  remote-ping entry(admin administrator, tag icmp) test result:
      Destination ip address:1.1.1.99
      Send operation times: 10              Receive response times: 10
      Min/Max/Average Round Trip Time: 2/5/2
      Square-Sum of Round Trip Time: 66
      Last complete test time: 2000-4-2 7:59:54.7
  Extend result:
      SD Maximal delay: 0                   DS Maximal delay: 0
```

```
    Packet lost in test: 0%
    Disconnect operation number: 0       Operation timeout number: 0
    System busy operation number: 0      Connection fail number: 0
    Operation sequence errors: 0         Drop operation number: 0
    Other operation errors: 0
[Sysname-remote-ping-administrator-icmp] display remote-ping history administrator icmp
  remote-ping entry(admin administrator, tag icmp) history record:
    Index     Response    Status     LasrRC      Time
        1            1         1          0    2004-11-25 16:28:55.0
        2            1         1          0    2004-11-25 16:28:55.0
        3            1         1          0    2004-11-25 16:28:55.0
        4            1         1          0    2004-11-25 16:28:55.0
        5            1         1          0    2004-11-25 16:28:55.0
        6            2         1          0    2004-11-25 16:28:55.0
        7            1         1          0    2004-11-25 16:28:55.0
        8            1         1          0    2004-11-25 16:28:55.0
        9            1         1          0    2004-11-25 16:28:55.9
       10            1         1          0    2004-11-25 16:28:55.9
```

Refer to the *remote-ping Command Manual* for detailed description on displayed information.

Table of Contents

1 IPv6 Configuration

When configuring IPv6, go to these sections for information you are interested in:

- IPv6 Overview
- IPv6 Configuration Task List
- IPv6 Configuration Example

Note

- The term "router" in this document refers to a router in a generic sense or an Ethernet switch running a routing protocol.
- The 3com switch 4500 supports IPv6 management features, but does not support IPv6 forwarding and related features.

IPv6 Overview

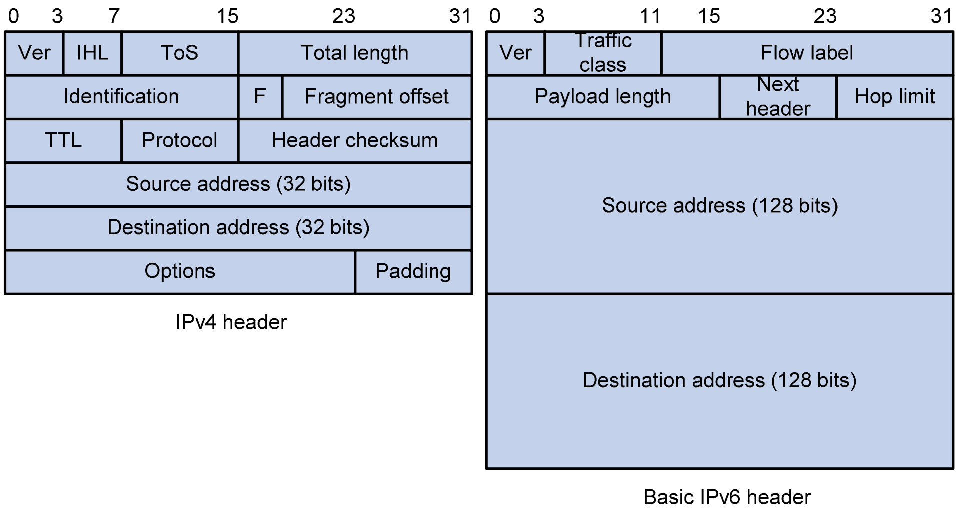
Internet Protocol Version 6 (IPv6), also called IP next generation (IPng), was designed by the Internet Engineering Task Force (IETF) as the successor to Internet Protocol Version 4 (IPv4). The significant difference between IPv6 and IPv4 is that IPv6 increases the IP address size from 32 bits to 128 bits.

IPv6 Features

Header format simplification

IPv6 cuts down some IPv4 header fields or moves them to extension headers to reduce the overhead of the basic IPv6 header. IPv6 uses a fixed-length header, thus making IPv6 packet handling simple and improving the forwarding efficiency. Although the IPv6 address size is four times that of IPv4 addresses, the size of the IPv6 header is only twice that of the IPv4 header (excluding the Options field). For the specific IPv6 header format, see Figure 1-1.

Figure 1-1 Comparison between IPv4 header format and IPv6 header format



Adequate address space

The source IPv6 address and the destination IPv6 address are both 128 bits (16 bytes) long. IPv6 can provide 3.4 x 10^{38} addresses to completely meet the requirements of hierarchical address division as well as allocation of public and private addresses.

Hierarchical address structure

IPv6 adopts the hierarchical address structure to quicken route search and reduce the system source occupied by the IPv6 routing table by means of route aggregation.

Automatic address configuration

To simplify the host configuration, IPv6 supports stateful address configuration and stateless address configuration.

- Stateful address configuration means that a host acquires an IPv6 address and related information from the server (for example, DHCP server).
- Stateless address configuration means that the host automatically configures an IPv6 address and related information based on its own link-layer address and the prefix information issued by the router.

In addition, a host can automatically generate a link-local address based on its own link-layer address and the default prefix (FE80::/64) to communicate with other hosts on the link.

Built-in security

IPv6 uses IPSec as its standard extension header to provide end-to-end security. This feature provides a standard for network security solutions and improves the interoperability between different IPv6 applications.

Support for QoS

The Flow Label field in the IPv6 header allows the device to label packets in a flow and provide special handling for these packets.

Enhanced neighbor discovery mechanism

The IPv6 neighbor discovery protocol is implemented by a group of Internet Control Message Protocol Version 6 (ICMPv6) messages. The IPv6 neighbor discovery protocol manages message exchange between neighbor nodes (nodes on the same link). The group of ICMPv6 messages takes the place of Address Resolution Protocol (ARP), Internet Control Message Protocol Version 4 (ICMPv4), and ICMPv4 redirect messages to provide a series of other functions.

Flexible extension headers

IPv6 cancels the Options field in IPv4 packets but introduces multiple extension headers. In this way, IPv6 enhances the flexibility greatly to provide scalability for IP while improving the processing efficiency. The Options field in IPv4 packets contains only 40 bytes, while the size of IPv6 extension headers is restricted by that of IPv6 packets.

Introduction to IPv6 Address

IPv6 addresses

An IPv6 address is represented as a series of 16-bit hexadecimals, separated by colons. An IPv6 address is divided into eight groups, 16 bits of each group are represented by four hexadecimal numbers which are separated by colons, for example, 2001:0000:130F:0000:0000:09C0:876A:130B.

To simplify the representation of IPv6 addresses, zeros in IPv6 addresses can be handled as follows:

- Leading zeros in each group can be removed. For example, the above-mentioned address can be represented in shorter format as 2001:0:130F:0:0:9C0:876A:130B.
- If an IPv6 address contains two or more consecutive groups of zeros, they can be replaced by the double-colon :: option. For example, the above-mentioned address can be represented in the shortest format as 2001:0:130F::9C0:876A:130B.

Caution

The double-colon :: can be used only once in an IPv6 address. Otherwise, the device is unable to determine how many zeros the double-colon represents when converting it to zeros to restore the IPv6 address to a 128-bit address.

An IPv6 address consists of two parts: address prefix and interface ID. The address prefix and the interface ID are respectively equivalent to the network ID and the host ID in an IPv4 address.

An IPv6 address prefix is written in IPv6-address/prefix-length notation, where IPv6-address is an IPv6 address in any of the notations and prefix-length is a decimal number indicating how many bits from the left of an IPv6 address are the address prefix.

IPv6 address classification

IPv6 addresses mainly fall into three types: unicast address, multicast address and anycast address.

- Unicast address: An identifier for a single interface, similar to an IPv4 unicast address .A packet sent to a unicast address is delivered to the interface identified by that address.

- Multicast address: An identifier for a set of interfaces (typically belonging to different nodes), similar to an IPv4 multicast address. A packet sent to a multicast address is delivered to all interfaces identified by that address.
- Anycast address: An identifier for a set of interfaces (typically belonging to different nodes).A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the nearest one, according to the routing protocols' measure of distance).

Note

There are no broadcast addresses in IPv6. Their function is superseded by multicast addresses.

The type of an IPv6 address is designated by the format prefix. Table 1-1 lists the mapping between major address types and format prefixes.

Table 1-1 Mapping between address types and format prefixes

Type		Format prefix (binary)	IPv6 prefix ID
Unicast address	Unassigned address	00...0 (128 bits)	::/128
	Loopback address	00...1 (128 bits)	::1/128
	Link-local address	1111111010	FE80::/10
	Site-local address	1111111011	FEC0::/10
	Global unicast address	other forms	—
Multicast address		11111111	FF00::/8
Anycast address		Anycast addresses are taken from unicast address space and are not syntactically distinguishable from unicast addresses.	

Unicast address

There are several forms of unicast address assignment in IPv6, including global unicast address, link-local address, and site-local address.

- The global unicast address, equivalent to an IPv4 public address, is used for aggregatable links and provided for network service providers. This type of address allows efficient routing aggregation to restrict the number of global routing entries.
- The link-local address is used in the neighbor discovery protocol and the stateless autoconfiguration process. Routers must not forward any packets with link-local source or destination addresses to other links.
- IPv6 unicast site-local addresses are similar to private IPv4 addresses. Routers must not forward any packets with site-local source or destination addresses outside of the site (equivalent to a private network).
- Loopback address: The unicast address 0:0:0:0:0:0:0:1 (represented in shorter format as ::1) is called the loopback address and may never be assigned to any physical interface. Like the loopback address in IPv4, it may be used by a node to send an IPv6 packet to itself.

- Unassigned address: The unicast address :: is called the unassigned address and may not be assigned to any node. Before acquiring a valid IPv6 address, a node may fill this address in the source address field of an IPv6 packet, but may not use it as a destination IPv6 address.

Multicast address

Multicast addresses listed in Table 1-2 are reserved for special purpose.

Table 1-2 Reserved IPv6 multicast addresses

Address	Application
FF01::1	Node-local scope all-nodes multicast address
FF02::1	Link-local scope all-nodes multicast address
FF01::2	Node-local scope all-routers multicast address
FF02::2	Link-local scope all-routers multicast address
FF05::2	Site-local scope all-routers multicast address

Besides, there is another type of multicast address: solicited-node address. The solicited-node multicast address is used to acquire the link-layer addresses of neighbor nodes on the same link and is also used for duplicate address detection. Each IPv6 unicast or anycast address has one corresponding solicited-node address. The format of a solicited-node multicast address is as follows:

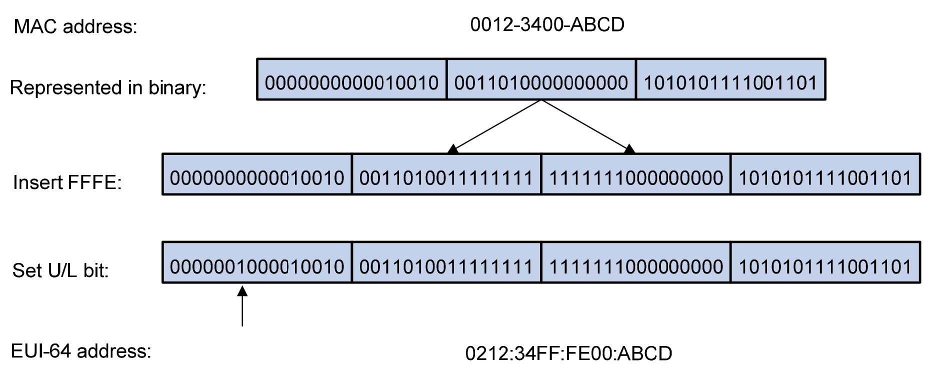
FF02:0:0:0:0:1:FFXX:XXXX

Where, FF02:0:0:0:0:1:FF is permanent and consists of 104 bits, and XX:XXXX is the last 24 bits of an IPv6 address.

Interface identifier in IEEE EUI-64 format

Interface identifiers in IPv6 unicast addresses are used to identify interfaces on a link and they are required to be unique on that link. Interface identifiers in IPv6 unicast addresses are currently required to be 64 bits long. An interface identifier is derived from the link-layer address of that interface. Interface identifiers in IPv6 addresses are 64 bits long, while MAC addresses are 48 bits long. Therefore, the hexadecimal number FFFE needs to be inserted in the middle of MAC addresses (behind the 24 high-order bits).To ensure the interface identifier obtained from a MAC address is unique, it is necessary to set the universal/local (U/L) bit (the seventh high-order bit) to "1". Thus, an interface identifier in EUI-64 format is obtained.

Figure 1-2 Convert a MAC address into an EUI-64 address



Introduction to IPv6 Neighbor Discovery Protocol

The IPv6 Neighbor Discovery Protocol (NDP) uses five types of ICMPv6 messages to implement the following functions:

- Address resolution
- Neighbor unreachability detection
- Duplicate address detection
- Router/prefix discovery
- Address autoconfiguration
- Redirection

Table 1-3 lists the types and functions of ICMPv6 messages used by the NDP.

Table 1-3 Types and functions of ICMPv6 messages

ICMPv6 message	Function
Neighbor solicitation (NS) message	Used to acquire the link-layer address of a neighbor
	Used to verify whether the neighbor is reachable
	Used to perform a duplicate address detection
Neighbor advertisement (NA) message	Used to respond to a neighbor solicitation message
	When the link layer address changes, the local node initiates a neighbor advertisement message to notify neighbor nodes of the change.
Router solicitation (RS) message	After started, a host sends a router solicitation message to request the router for an address prefix and other configuration information for the purpose of autoconfiguration.
Router advertisement (RA) message	Used to respond to a router solicitation message
	With the RA message suppression disabled, the router regularly sends a router advertisement message containing information such as address prefix and flag bits.
Redirect message	When a certain condition is satisfied, the default gateway sends a redirect message to the source host so that the host can reselect a correct next hop router to forward packets.

Note

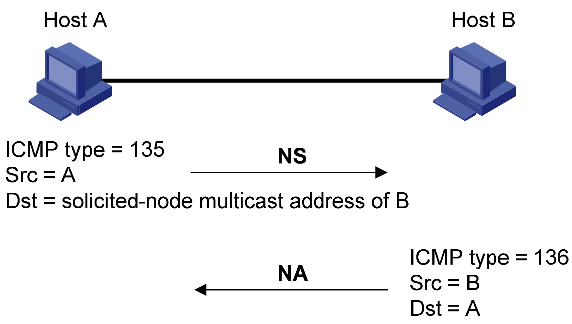
- The 3com switch 4500 does not support the RS, RA, or Redirect message.
- Of the above mentioned IPv6 NDP functions, 3com switches 4500 support the following three functions: address resolution, neighbor unreachability detection, and duplicate address detection. The subsequent sections present a detailed description of these three functions and relevant configuration.

The NDP mainly provides the following functions:

Address resolution

Similar to the ARP function in IPv4, a node acquires the link-layer address of neighbor nodes on the same link through NS and NA messages. Figure 1-3 shows how node A acquires the link-layer address of node B.

Figure 1-3 Address resolution



The address resolution procedure is as follows:

1) Node A multicasts an NS message. The source address of the NS message is the IPv6 address of the interface of node A and the destination address is the solicited-node multicast address of node B. The NS message contains the link-layer address of node A.
2) After receiving the NS message, node B judges whether the destination address of the packet is the corresponding solicited-node multicast address of its own IPv6 address. If yes, node B learns the link-layer address of node A and returns an NA message containing the link-layer address of node B in the unicast mode.
3) Node A acquires the link-layer address of node B from the NA message. After that, node A and node B can communicate with each other.

Neighbor unreachability detection

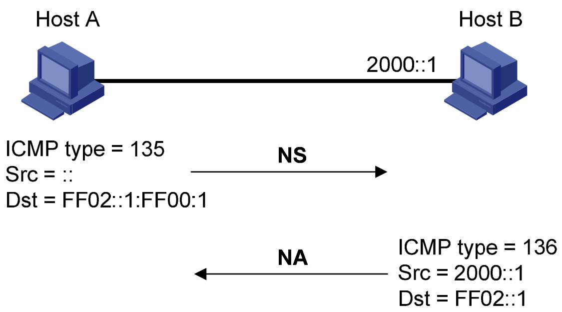
After node A acquires the link-layer address of its neighbor node B, node A can verify whether node B is reachable according to NS and NA messages.

1) Node A sends an NS message whose destination address is the IPv6 address of node B.
2) If node A receives an NA message from node B, node A considers that node B is reachable. Otherwise, node B is unreachable.

Duplicate address detection

After a node acquires an IPv6 address, it should perform the duplicate address detection to determine whether the address is being used by other nodes (similar to the gratuitous ARP function). The duplication address detection is accomplished through NS and NA messages. Figure 1-4 shows the duplicate address detection procedure.

Figure 1-4 Duplicate address detection



The duplicate address detection procedure is as follows:

1) Node A sends an NS message whose source address is the unassigned address :: and the destination address is the corresponding solicited-node multicast address of the IPv6 address to be detected. The NS message also contains the IPv6 address.
2) If node B uses this IPv6 address, node B returns an NA message. The NA message contains the IPv6 address of node B.
3) Node A learns that the IPv6 address is being used by node B after receiving the NA message from node B. Otherwise, node B is not using the IPv6 address and node A can use it.

Protocols and Standards

Protocol specifications related to IPv6 include:

- RFC 1881: IPv6 Address Allocation Management
- RFC 1887: An Architecture for IPv6 Unicast Address Allocation
- RFC 1981: Path MTU Discovery for IP version 6
- RFC 2375: IPv6 Multicast Address Assignments
- RFC 2460: Internet Protocol, Version 6 (IPv6) Specification.
- RFC 2461: Neighbor Discovery for IP Version 6 (IPv6)
- RFC 2462: IPv6 Stateless Address Autoconfiguration
- RFC 2463: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification
- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks
- RFC 2526: Reserved IPv6 Subnet Anycast Addresses
- RFC 3307: Allocation Guidelines for IPv6 Multicast Addresses
- RFC 3513: Internet Protocol Version 6 (IPv6) Addressing Architecture

IPv6 Configuration Task List

Complete the following tasks to configure IPv6:

Task	Remarks
Configuring an IPv6 Unicast Address	Required
Configuring IPv6 NDP	Optional
Configuring a Static IPv6 Route	Optional
Configuring IPv6 TCP Properties	Optional

Task	Remarks
Configuring the Maximum Number of IPv6 ICMP Error Packets Sent within a Specified Time	Optional
Configuring the Hop Limit of ICMPv6 Reply Packets	Optional
Displaying and Maintaining IPv6	Optional

Configuring an IPv6 Unicast Address

- An IPv6 address is required for a host to access an IPv6 network. A host can be assigned a global unicast address, a site-local address, or a link-local address.
- To enable a host to access a public IPv6 network, you need to assign an IPv6 global unicast address to it.

IPv6 site-local addresses and global unicast addresses can be configured in either of the following ways:

- EUI-64 format: When the EUI-64 format is adopted to form IPv6 addresses, the IPv6 address prefix of an interface is the configured prefix and the interface identifier is derived from the link-layer address of the interface.
- Manual configuration: IPv6 site-local addresses or global unicast addresses are configured manually.

IPv6 link-local addresses can be acquired in either of the following ways:

- Automatic generation: The device automatically generates a link-local address for an interface according to the link-local address prefix (FE80::/64) and the link-layer address of the interface.
- Manual assignment: IPv6 link-local addresses can be assigned manually.

Follow these steps to configure an IPv6 unicast address:

<table>
<tr><th colspan="2">To do...</th><th>Use the command...</th><th>Remarks</th></tr>
<tr><td colspan="2">Enter system view</td><td>system-view</td><td>—</td></tr>
<tr><td colspan="2">Enter VLAN interface view</td><td>interface interface-type interface-number</td><td>—</td></tr>
<tr><td rowspan="2">Configure an IPv6 global unicast address or site-local address</td><td>Manually assign an IPv6 address</td><td>ipv6 address { ipv6-address prefix-length | ipv6-address/prefix-length }</td><td rowspan="2">Use either command
By default, no site-local address or global unicast address is configured for an interface.
Note that the prefix specified by the prefix-length argument in an EUI-64 address cannot exceed 64 bits in length.</td></tr>
<tr><td>Adopt the EUI-64 format to form an IPv6 address</td><td>ipv6 address ipv6-address/prefix-length eui-64</td></tr>
</table>

To do...		Use the command...	Remarks
Configure an IPv6 link-local address	Automatically generate a link-local address	**ipv6 address auto link-local**	Optional By default, after an IPv6 site-local address or global unicast address is configured for an interface, a link-local address will be generated automatically.
	Manually assign a link-local address for an interface.	**ipv6 address** *ipv6-address* **link-local**	

Note

- If XRN fabric ports are configured on a 3com switch 4500, no IPv6 address can be configured for the switch.
- IPv6 unicast addresses can be configured for only one VLAN interface on a 3com switch 4500. The total number of global unicast addresses and site-local addresses on the VLAN interface can be up to four.
- After an IPv6 site-local address or global unicast address is configured for an interface, a link-local address will be generated automatically. The automatically generated link-local address is the same as the one generated by using the **ipv6 address auto link-local** command.
- The manual assignment takes precedence over the automatic generation. That is, if you first adopt the automatic generation and then the manual assignment, the manually assigned link-local address will overwrite the automatically generated one. If you first adopt the manual assignment and then the automatic generation, the automatically generated link-local address will not take effect and the link-local address of an interface is still the manually assigned one. If the manually assigned link-local address is deleted, the automatically generated link-local address takes effect.
- You must have carried out the **ipv6 address auto link-local** command before you carry out the **undo ipv6 address auto link-local** command. However, if an IPv6 site-local address or global unicast address is already configured for an interface, the interface still has a link-local address because the system automatically generates one for the interface. If no IPv6 site-local address or global unicast address is configured, the interface has no link-local address.

Configuring IPv6 NDP

Configuring a static neighbor entry

The IPv6 address of a neighbor node can be resolved into a link-layer address dynamically through NS and NA messages or statically through manual configuration.

You can configure a static neighbor entry in two ways:

- Mapping a VLAN interface to an IPv6 address and a link-layer address
- Mapping a port in a VLAN to an IPv6 address and a link-layer address

If you configure a static neighbor entry in the second way, make sure the corresponding VLAN interface exists. In this case, the device associates the VLAN interface to the IPv6 address to uniquely identify a static neighbor entry.

Follow these steps to configure a static neighbor entry:

To do...	Use the command...	Remarks
Enter system view	**system-view**	—
Configure a static neighbor entry	**ipv6 neighbor** *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }	Required

Configuring the maximum number of neighbors dynamically learned

The device can dynamically acquire the link-layer address of a neighbor node through NS and NA messages and add it to the neighbor table. Too large a neighbor table may lead to the forwarding performance degradation of the device. Therefore, you can restrict the size of the neighbor table by setting the maximum number of neighbors that an interface can dynamically learn. When the number of dynamically learned neighbors reaches the threshold, the interface will stop learning neighbor information.

Follow these steps to configure the maximum number of neighbors dynamically learned:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface** *interface-type interface-number*	—
Configure the maximum number of neighbors dynamically learned by an interface	**ipv6 neighbors max-learning-num** *number*	Optional The default value is 2,048

Configuring the attempts to send an ns message for duplicate address detection

The device sends a neighbor solicitation (NS) message for duplicate address detection. If the device does not receive a response within a specified time (set by the **ipv6 nd ns retrans-timer** command), the device continues to send an NS message. If the device still does not receive a response after the number of attempts to send an NS message reaches the maximum, the device judges the acquired address is available.

Follow these steps to configure the attempts to send an NS message for duplicate address detection:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface** *interface-type interface-number*	—
Configure the attempts to send an NS message for duplicate address detection	**ipv6 nd dad attempts** *value*	Optional 1 by default. When the *value* argument is set to 0, the duplicate address detection is disabled.

Configuring the NS Interval

After a device sends an NS message, if it does not receive a response within a specific period, the device will send another NS message. You can configure the interval for sending NS messages.

Follow these steps to configure the NS interval:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface** *interface-type interface-number*	—
Specify the NS interval	**ipv6 nd ns retrans-timer** *value*	Optional 1,000 milliseconds by default.

Configuring the neighbor reachable timeout time on an interface

After a neighbor passed the reachability detection, the device considers the neighbor to be reachable in a specific period. However, the device will examine whether the neighbor is reachable again when there is a need to send packets to the neighbor after the neighbor reachable timeout time elapsed.

Follow these steps to configure the neighbor reachable timeout time on an interface:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enter VLAN interface view	**interface** *interface-type interface-number*	—
Configure the neighbor reachable timeout time	**ipv6 nd nud reachable-time** *value*	Optional 30,000 milliseconds by default.

Configuring a Static IPv6 Route

You can configure static IPv6 routes for network interconnection in a small sized IPv6 network.

Follow these steps to configure a static IPv6 route:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure a static IPv6 route	**ipv6 route-static** *ipv6-address prefix-length* [*interface-type interface-number*] *nexthop-address*	Required By default, no static IPv6 route is configured.

Configuring IPv6 TCP Properties

The IPv6 TCP properties you can configure include:

- synwait timer: When a SYN packet is sent, the synwait timer is triggered. If no response packet is received before the synwait timer expires, the IPv6 TCP connection establishment fails.
- finwait timer: When the IPv6 TCP connection status is FIN_WAIT_2, the finwait timer is triggered. If no packet is received before the finwait timer expires, the IPv6 TCP connection is terminated. If FIN

packets are received, the IPv6 TCP connection status becomes TIME_WAIT. If other packets are received, the finwait timer is reset from the last packet and the connection is terminated after the finwait timer expires.

- Size of IPv6 TCP receiving/sending buffer.

Follow these steps to configure IPv6 TCP properties:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the finwait timer of IPv6 TCP packets	**tcp ipv6 timer fin-timeout** *wait-time*	Optional 675 seconds by default.
Set the synwait timer of IPv6 TCP packets	**tcp ipv6 timer syn-timeout** *wait-time*	Optional 75 seconds by default.
Configure the size of IPv6 TCP receiving/sending buffer	**tcp ipv6 window size**	Optional 8 KB by default.

Configuring the Maximum Number of IPv6 ICMP Error Packets Sent within a Specified Time

If too many IPv6 ICMP error packets are sent within a short time in a network, network congestion may occur. To avoid network congestion, you can control the maximum number of IPv6 ICMP error packets sent within a specified time. Currently, the token bucket algorithm is adopted.

You can set the capacity of a token bucket, namely, the number of tokens in the bucket. In addition, you can set the update period of the token bucket, namely, the interval for updating the number of tokens in the token bucket to the configured capacity. One token allows one IPv6 ICMP error packet to be sent. Each time an IPv6 ICMP error packet is sent, the number of tokens in a token bucket decreases by 1. If the number of the IPv6 ICMP error packets that are continuously sent out reaches the capacity of the token bucket, the subsequent IPv6 ICMP error packets cannot be sent out until new tokens are put into the token bucket based on the specified update frequency.

Follow these steps to configure the maximum number of IPv6 ICMP error packets sent within a specified time:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the maximum number of IPv6 ICMP error packets sent within a specified time	**ipv6 icmp-error** { **bucket** *bucket-size* | **ratelimit** *interval* }*	Optional By default, the capacity of a token bucket is 10 and the update period to 100 milliseconds. That is, at most 10 IPv6 ICMP error packets can be sent within an update period.

Configuring the Hop Limit of ICMPv6 Reply Packets

When sending an ICMPv6 reply packet, the device will fill a configurable value in the Hop Limit field in the ICMPv6 reply packet header.

Follow these steps to configure the hop limit of ICMPv6 reply packets:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Configure the hop limit of ICMPv6 reply packets	**ipv6 nd hop-limit** *value*	Optional 64 by default.

Displaying and Maintaining IPv6

To do…	Use the command…	Remarks
Display the FIB entries	**display ipv6 fib**	Available in any view
Display the mapping between host name and IPv6 address	**display ipv6 host**	
Display the brief IPv6 information of an interface	**display ipv6 interface** [*interface-type interface-number* | **brief**]	
Display neighbor information	**display ipv6 neighbors** [*ipv6-address* | **all** | **dynamic** | **interface** *interface-type interface-number* | **static** | **vlan** *vlan-id*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	
Display the total number of neighbor entries satisfying the specified conditions	**display ipv6 neighbors** { **all** | **dynamic** | **static** | **interface** *interface-type interface-number* | **vlan** *vlan-id* } **count**	
Display information about the routing table	**display ipv6 route-table** [**verbose**]	
Display information related to a specified socket	**display ipv6 socket** [**socktype** *socket-type*] [*task-id socket-id*]	
Display the statistics of IPv6 packets and IPv6 ICMP packets	**display ipv6 statistics**	
Display the statistics of IPv6 TCP packets	**display tcp ipv6 statistics**	
Display the IPv6 TCP connection status	**display tcp ipv6 status**	
Display the statistics of IPv6 UDP packets	**display udp ipv6 statistics**	
Clear IPv6 neighbor information	**reset ipv6 neighbors** [**all** | **dynamic** | **interface** *interface-type interface-number* | **static**]	Available in user view
Clear the statistics of IPv6 packets	**reset ipv6 statistics**	
Clear the statistics of all IPv6 TCP packets	**reset tcp ipv6 statistics**	
Clear the statistics of all IPv6 UDP packets	**reset udp ipv6 statistics**	

IPv6 Configuration Example

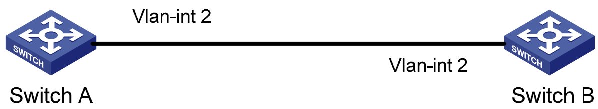
IPv6 Unicast Address Configuration

Network requirements

Two switches are directly connected through two Ethernet ports. The Ethernet ports belong to VLAN 2. Different types of IPv6 addresses are configured for the interface VLAN-interface 2 on each switch to verify the connectivity between the two switches. The IPv6 prefix in the EUI-64 format is 2001::/64, the global unicast address of Switch A is 3001::1/64, and the global unicast address of Switch B is 3001::2/64.

Network diagram

Figure 1-5 Network diagram for IPv6 address configuration



Configuration procedure

1) Configure Switch A.

Configure an automatically generated link-local address for the interface VLAN-interface 2.

```
<SwitchA> system-view
[SwitchA] interface Vlan-interface 2
[SwitchA-Vlan-interface2] ipv6 address auto link-local
```

Configure an EUI-64 address for the interface VLAN-interface 2.

```
[SwitchA-Vlan-interface2] ipv6 address 2001::/64 eui-64
```

Configure a global unicast address for the interface VLAN-interface 2.

```
[SwitchA-Vlan-interface2] ipv6 address 3001::1/64
```

2) Configure Switch B.

Configure an automatically generated link-local address for the interface VLAN-interface 2.

```
<SwitchA> system-view
[SwitchB] interface Vlan-interface 2
[SwitchB-Vlan-interface2] ipv6 address auto link-local
```

Configure an EUI-64 address for the interface VLAN-interface 2.

```
[SwitchB-Vlan-interface2] ipv6 address 2001::/64 eui-64
```

Configure a global unicast address for the interface VLAN-interface 2.

```
[SwitchB-Vlan-interface2] ipv6 address 3001::2/64
```

Verification

Display the brief IPv6 information of an interface on Switch A.

```
[SwitchA-Vlan-interface2] display ipv6 interface vlan-interface 2
Vlan-interface2 current state : UP
Line protocol current state : UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE49:8048
```

```
  Global unicast address(es):
    2001::20F:E2FF:FE49:8048, subnet is 2001::/64
    3001::1, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF49:8048
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Display the brief IPv6 information of the interface on Switch B.

```
[SwitchB-Vlan-interface2] display ipv6 interface Vlan-interface 2
Vlan-interface2 current state : UP
Line protocol current state : UP
IPv6 is enabled, link-local address is FE80::20F:E2FF:FE00:1
  Global unicast address(es):
    2001::20F:E2FF:FE00:1, subnet is 2001::/64
    3001::2, subnet is 3001::/64
  Joined group address(es):
    FF02::1:FF00:2
    FF02::1:FF00:1
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

On Switch A, ping the link-local address, EUI-64 address, and global unicast address of Switch B. If the configurations are correct, the above three types of IPv6 addresses can be pinged.

Caution

When you use the **ping ipv6** command to verify the reachability of the destination, you must specify the "**–i**" keyword if the destination address is a link-local address. For the operation of IPv6 ping, refer to section IPv6 Ping.

```
[SwitchA-Vlan-interface2] ping ipv6 FE80::20F:E2FF:FE00:1 -i Vlan-interface 2
  PING FE80::20F:E2FF:FE00:1 : 56  data bytes, press CTRL_C to break
    Reply from FE80::20F:E2FF:FE00:1
    bytes=56 Sequence=1 hop limit=255  time = 80 ms
    Reply from FE80::20F:E2FF:FE00:1
    bytes=56 Sequence=2 hop limit=255  time = 60 ms
```

```
    Reply from FE80::20F:E2FF:FE00:1
    bytes=56 Sequence=3 hop limit=255  time = 60 ms
    Reply from FE80::20F:E2FF:FE00:1
    bytes=56 Sequence=4 hop limit=255  time = 70 ms
    Reply from FE80::20F:E2FF:FE00:1
    bytes=56 Sequence=5 hop limit=255  time = 60 ms
  --- FE80::20F:E2FF:FE00:1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 60/66/80 ms

[SwitchA-Vlan-interface2] ping ipv6 2001::20F:E2FF:FE00:1
  PING 2001::20F:E2FF:FE00:1 : 56  data bytes, press CTRL_C to break
    Reply from 2001::20F:E2FF:FE00:1
    bytes=56 Sequence=1 hop limit=255  time = 40 ms
    Reply from 2001::20F:E2FF:FE00:1
    bytes=56 Sequence=2 hop limit=255  time = 70 ms
    Reply from 2001::20F:E2FF:FE00:1
    bytes=56 Sequence=3 hop limit=255  time = 60 ms
    Reply from 2001::20F:E2FF:FE00:1
    bytes=56 Sequence=4 hop limit=255  time = 60 ms
    Reply from 2001::20F:E2FF:FE00:1
    bytes=56 Sequence=5 hop limit=255  time = 60 ms

  --- 2001::20F:E2FF:FE00:1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/58/70 ms

[SwitchA-Vlan-interface2] ping ipv6 3001::2
  PING 3001::2 : 56  data bytes, press CTRL_C to break
    Reply from 3001::2
    bytes=56 Sequence=1 hop limit=255  time = 50 ms
    Reply from 3001::2
    bytes=56 Sequence=2 hop limit=255  time = 60 ms
    Reply from 3001::2
    bytes=56 Sequence=3 hop limit=255  time = 60 ms
    Reply from 3001::2
    bytes=56 Sequence=4 hop limit=255  time = 70 ms
    Reply from 3001::2
    bytes=56 Sequence=5 hop limit=255  time = 60 ms

  --- 3001::2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
0.00% packet loss
round-trip min/avg/max = 50/60/70 ms
```

2 IPv6 Application Configuration

When configuring IPv6 application, go to these sections for information you are interested in:

- Introduction to IPv6 Application
- Configuring IPv6 Application
- IPv6 Application Configuration Example
- Troubleshooting IPv6 Application

Introduction to IPv6 Application

IPv6 are supporting more and more applications. Most of IPv6 applications are the same as those of IPv4. The applications supported on 3com switch 4500 are:

- Ping
- Traceroute
- TFTP
- Telnet

Configuring IPv6 Application

IPv6 Ping

The **ping ipv6** command is commonly used for testing the reachability of a host. This command sends an ICMPv6 message to the destination host and records the time for the response message to be received. For details about the **ping** command, refer to *System Maintenance and Debugging Operation* in this manual.

After you execute the **ping ipv6** command, you can press **Ctrl+C** to terminate the ping operation.

Follow these steps to ping IPv6:

To do…	Use the command…	Remarks
Ping IPv6	**ping ipv6** [**-a** *source-ipv6* | **-c** *count* | **-m** *interval* | **-s** *packet-size* | **-t** *timeout*]* *remote-system* [**-i** *interface-type interface-number*]	Required Available in any view

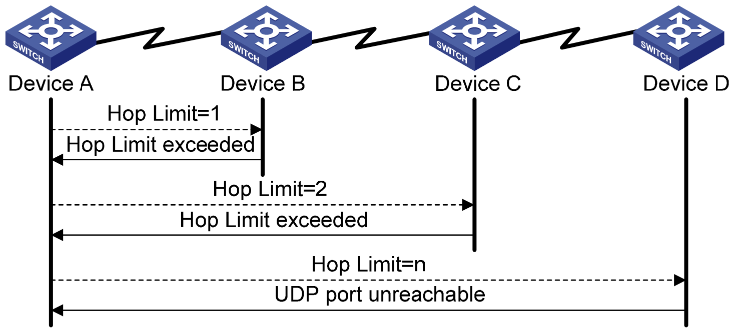
Caution

When you use the **ping ipv6** command to verify the reachability of the destination, you must specify the "**–i**" keyword if the destination address is a link-local address.

IPv6 Traceroute

The **traceroute ipv6** command is used to record the route of IPv6 packets from source to destination, so as to check whether the link is available and determine the point of failure.

Figure 2-1 Traceroute process



As Figure 2-1 shows, the traceroute process is as follows:

- The source sends an IP datagram with the Hop Limit of 1.
- If the first hop device receiving the datagram reads the Hop Limit of 1, it will discard the packet and return an ICMP timeout error message. Thus, the source can get the first device's address in the route.
- The source sends a datagram with the Hop Limit of 2 and the second hop device returns an ICMP timeout error message. The source gets the second device's address in the route.
- This process continues until the datagram reaches the destination host. As there is no application using the UDP port, the destination returns a "port unreachable" ICMP error message.
- The source receives the "port unreachable" ICMP error message and understands that the packet has reached the destination, and thus determines the route of the packet from source to destination.

Follow these steps to traceroute IPv6:

To do…	Use the command…	Remarks
Traceroute IPv6	**tracert ipv6** [**-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-num* | **-w** *timeout*]* *remote-system*	Required Available in any view

IPv6 TFTP

IPv6 supports Trivial File Transfer Protocol (TFTP). As a client, the device can download files from or upload files to a TFTP server. For details about TFTP, see *FTP-SFTP-TFTP Operation*.

Configuration preparation

Enable TFTP on the TFTP server and specify the path to download or upload files. For specific operations, refer to TFTP server configuration specifications.

IPv6 TFTP configuration

Follow these steps to download or upload files to TFTP servers:

To do…	Use the command…	Remarks
Download/Upload files from TFTP server	**tftp ipv6** *remote-system* [**-i** *interface-type* *interface-number*] { **get** | **put** } *source-filename* [*destination-filename*]	Required Available in user view

Caution

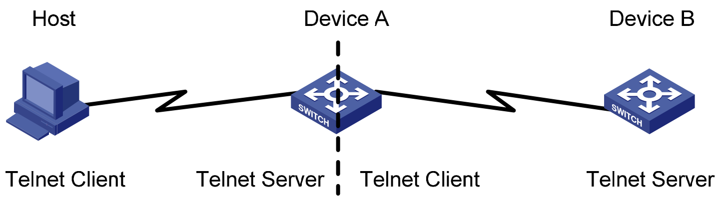
When you use the **tftp ipv6** command to connect to the TFTP server, you must specify the "–**i**" keyword if the destination address is a link-local address.

IPv6 Telnet

Telnet protocol belongs to application layer protocols of the TCP/IP protocol suite, and is used to provide remote login and virtual terminals. The device can be used either as a Telnet client or a Telnet server.

As the following figure shows, the Host is running Telnet client application of IPv6 to set up an IPv6 Telnet connection with Device A, which serves as the Telnet server. If Device A again connects to Device B through Telnet, the Device A is the Telnet client and Device B is the Telnet server.

Figure 2-2 Provide Telnet services



Configuration prerequisites

Enable Telnet on the Telnet server and configure the authentication method. For details, refer to *Login Operation* in this manual.

Follow these steps to set up IPv6 Telnet connections:

To do…	Use the command…	Remarks
Perform the **telnet** command on the Telnet client to log in to other devices	**telnet ipv6** *remote-system* [**-i** *interface-type interface-number*] [*port-number*]	Required Available in user view

Caution

When you use the **telnet ipv6** command to connect to the Telnet server, you must specify the "–**i**" keyword if the destination address is a link-local address.

Displaying and maintaining IPv6 Telnet

To do…	Use the command…	Remarks
Display the use information of the users who have logged in	**display users** [**all**]	Available in any view

IPv6 Application Configuration Example

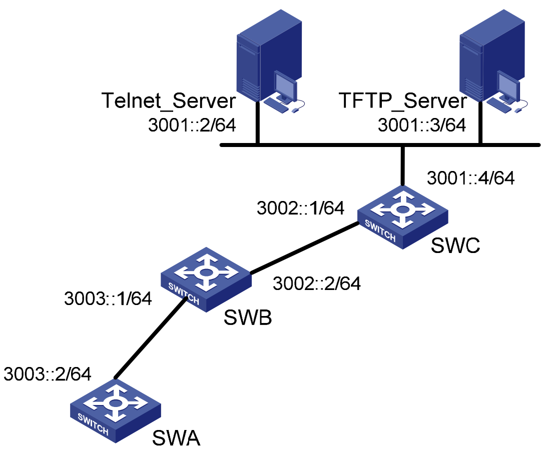
IPv6 Applications

Network requirements

In Figure 2-3, SWA, SWB, and SWC are three switches, among which SWA is a 3com switch 4500, SWB and SWC are two switches supporting IPv6 forwarding. In a LAN, there is a Telnet server and a TFTP server for providing Telnet service and TFTP service to the switch respectively. It is required that you telnet to the telnet server from SWA and download files from the TFTP server.

Network diagram

Figure 2-3 Network diagram for IPv6 applications



Configuration procedure

Note

You need configure IPv6 address at the switch's and server's interfaces and ensure that the route between the switch and the server is accessible before the following configuration.

Ping SWB's IPv6 address from SWA.

```
<SWA> ping ipv6 3003::1
  PING 3003::1 : 64  data bytes, press CTRL_C to break
    Reply from 3003::1
    bytes=56 Sequence=1 hop limit=64  time = 110 ms
    Reply from 3003::1
```

```
    bytes=56 Sequence=2 hop limit=64  time = 31 ms
    Reply from 3003::1
    bytes=56 Sequence=3 hop limit=64  time = 31 ms
    Reply from 3003::1
    bytes=56 Sequence=4 hop limit=64  time = 31 ms
    Reply from 3003::1
    bytes=56 Sequence=5 hop limit=64  time = 31 ms

--- 3003::1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
    round-trip min/avg/max = 31/46/110 ms
```

On SWA, configure static routes to SWC, the Telnet Server, and the TFTP Server.

```
<SWA> system-view
[SWA] ipv6 route-static 3002:: 64 3003::1
[SWA] ipv6 route-static 3001:: 64 3003::1
[SWA] quit
```

Trace the IPv6 route from SWA to SWC.

```
<SWA> tracert ipv6 3002::1
 traceroute to 3002::1  30 hops max,60 bytes packet
 1  3003::1 30 ms  0 ms  0 ms
 2  3002::1 10 ms 10 ms 0 ms
```

SWA downloads a file from TFTP server 3001::3.

```
<SWA> tftp ipv6 3001::3 get filetoget flash:/filegothere
  .
  File will be transferred in binary mode
  Downloading file from remote tftp server, please wait....
  TFTP:       13 bytes received in 1.243 second(s)
  File downloaded successfully.
```

SWA Connect to Telnet server 3001::2.

```
<SWA> telnet ipv6 3001::2
Trying 3001::2...
Press CTRL+K to abort
Connected to 3001::2 ...
Telnet Server>
```

Troubleshooting IPv6 Application

Unable to Ping a Remote Destination

Symptom

Unable to ping a remote destination and return an error message.

Solution

- Check that the IPv6 addresses are configured correctly.
- Use the **display ipv6 interface** command to determine the interfaces of the source and the destination and the link-layer protocol between them are up.
- Use the **display ipv6 route-table** command to verify that the destination is reachable.
- Use the **ping ipv6 -t** *timeout* { *destination-ipv6-address* | *hostname* } [**-i** *interface-type interface-number*] command to increase the timeout time limit, so as to determine whether it is due to the timeout limit is too small.

Unable to Run Traceroute

Symptom

Unable to trace the route by performing traceroute operations.

Solution

- Check that the destination host can be pinged.
- If the host can be pinged through, check whether the UDP port that was included in the **tracert ipv6** command is used by an application on the host. If yes, you need to use the **tracert ipv6** command with an unreachable UDP port.

Unable to Run TFTP

Symptom

Unable to download and upload files by performing TFTP operations.

Solution

- Check that the route between the device and the TFTP server is up.
- Check that the file system of the device is usable. You can check it by running the **dir** command in user view.
- Check that the ACL configured for the TFTP server does not block the connection to the TFTP server.

Unable to Run Telnet

Symptom

Unable to login to Telnet server by performing Telnet operations.

Solution

- Check that the Telnet server application is running on the server. Check the configuration allows the server reachable.
- Check that the route between the device and the TFTP server is up.

Table of Contents

1 Access Management Configuration

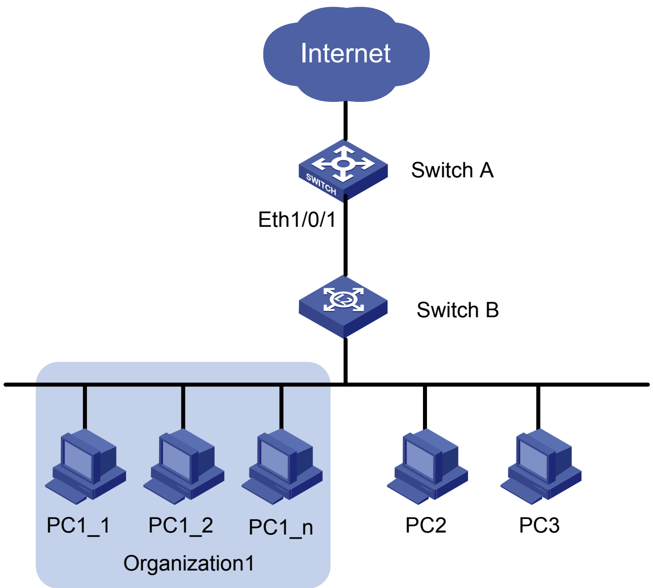
When configuring access management, go to these sections for information you are interested in:

- Access Management Overview
- Configuring Access Management
- Access Management Configuration Examples

Access Management Overview

Normally, client PCs in a network are connected to switches operating on the network access layer (also referred to as access switches) through Layer 2 switches; and the access switches provide external network accesses for the client PCs through their upstream links. In the network shown in Figure 1-1, Switch A is an access switch; Switch B is a Layer 2 switch.

Figure 1-1 Typical Ethernet access networking scenario



The access management function aims to manage user access rights on access switches. It enables you to manage the external network access rights of the hosts connected to ports of an access switch.

To implement the access management function, you need to configure an IP address pool on a port of an access switch, that is, bind a specified range of IP addresses to the port.

- A port with an access management IP address pool configured only allows the hosts with their IP addresses in the access management IP address pool to access external networks.

- A port without an access management IP address pool configured allows the hosts to access external networks only if their IP addresses are not in the access management IP address pools of other ports of the switch.

Note that the IP addresses in the access management IP address pool configured on a port must be in the same network segment as the IP address of the VLAN (where the port belongs to) interface.

Configuring Access Management

Follow these steps to configure access management:

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Enable access management function	**am enable**	Required By default, the system disables the access management function.
Enable access management trap	**am trap enable**	Required By default, access management trap is disabled
Enter Ethernet port view	**interface** *interface-type interface-number*	—
Configure the access management IP address pool of the port	**am ip-pool** *address-list*	Required By default, no access management IP address pool is configured.
Display current configuration of access management	**display am** [*interface-list*]	Execute this command in any view.

Note

- Before configuring the access management IP address pool of a port, you need to configure the interface IP address of the VLAN to which the port belongs, and the IP addresses in the access management IP address pool of a port must be in the same network segment as the interface IP address of the VLAN which the port belongs to.
- If an access management address pool configured contains IP addresses that belong to the static ARP entries of other ports, the system prompts you to delete the corresponding static ARP entries to ensure the access management IP address pool can take effect.
- To allow only the hosts with their IP addresses in the access management address pool of a port to access external networks, do not configure static ARP entries for IP addresses not in the IP address pool.

Access Management Configuration Examples

Access Management Configuration Example

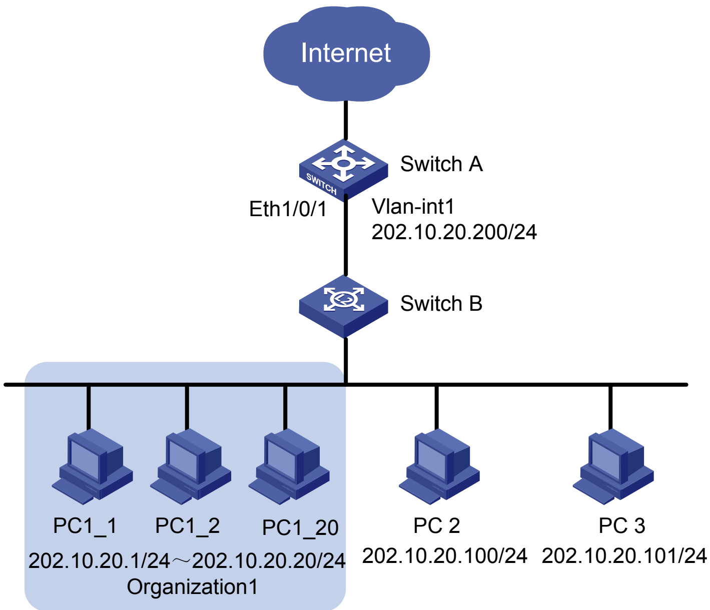
Network requirements

Client PCs are connected to the external network through Switch A (an Ethernet switch). The IP addresses of the PCs of Organization 1 are in the range 202.10.20.1/24 to 202.10.20.20/24. The IP address of PC 2 is 202.10.20.100/24, and that of PC 3 is 202.10.20.101/24.

- Allow the PCs of Organization 1 to access the external network through Ethernet 1/0/1 on Switch A. The port belongs to VLAN 1, and the IP address of VLAN-interface 1 is 202.10.20.200/24.
- Disable the PCs that are not of Organization 1 (PC 2 and PC 3) from accessing the external network through Ethernet 1/0/1 of Switch A.

Network diagram

Figure 1-2 Network diagram for access management configuration



Configuration procedure

Perform the following configuration on Switch A.

Enable access management.

```
<Sysname> system-view
[Sysname] am enable
```

Set the IP address of VLAN-interface 1 to 202.10.20.200/24.

```
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address 202.10.20.200 24
[Sysname-Vlan-interface1] quit
```

Configure the access management IP address pool on Ethernet 1/0/1.

```
[Sysname] interface Ethernet 1/0/1
```

```
[Sysname-Ethernet1/0/1] am ip-pool 202.10.20.1 20
```

Combining Access Management with Port Isolation

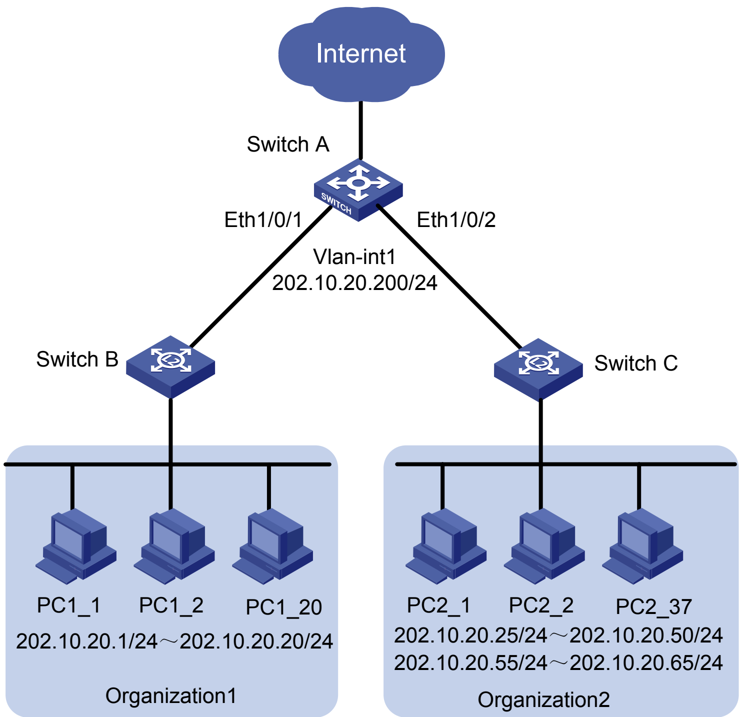
Network requirements

Client PCs are connected to the external network through Switch A (an Ethernet switch). The IP addresses of the PCs of Organization 1 are in the range 202.10.20.1/24 to 202.10.20.20/24, and those of the PCs in Organization 2 are in the range 202.10.20.25/24 to 202.10.20.50/24 and the range 202.10.20.55 to 202.10.20.65/24.

- Allow the PCs of Organization 1 to access the external network through Ethernet 1/0/1 of Switch A.
- Allow the PCs of Organization 2 to access the external network through Ethernet 1/0/2 of Switch A.
- Ethernet 1/0/1 and Ethernet 1/0/2 belong to VLAN 1. The IP address of VLAN-interface 1 is 202.10.20.200/24.
- PCs of Organization 1 are isolated from those of Organization 2 on Layer 2.

Network diagram

Figure 1-3 Network diagram for combining access management and port isolation



Configuration procedure

Perform the following configuration on Switch A.

For information about port isolation and the corresponding configuration, refer to the *Port Isolation Operation*.

Enable access management.

```
<Sysname> system-view
[Sysname] am enable
```

Set the IP address of VLAN-interface 1 to 202.10.20.200/24.

```
[Sysname] interface Vlan-interface 1
[Sysname-Vlan-interface1] ip address 202.10.20.200 24
[Sysname-Vlan-interface1] quit
```

Configure the access management IP address pool on Ethernet 1/0/1.

```
[Sysname] interface Ethernet 1/0/1
[Sysname-Ethernet1/0/1] am ip-pool 202.10.20.1 20
```

Add Ethernet 1/0/1 to the port isolation group.

```
[Sysname-Ethernet1/0/1] port isolate
[Sysname-Ethernet1/0/1] quit
```

Configure the access management IP address pool on Ethernet 1/0/2.

```
[Sysname] interface Ethernet 1/0/2
[Sysname-Ethernet1/0/2] am ip-pool 202.10.20.25 26 202.10.20.55 11
```

Add Ethernet 1/0/2 to the port isolation group.

```
[Sysname-Ethernet1/0/2] port isolate
[Sysname-Ethernet1/0/2] quit
```

Table of Contents

Appendix A Acronyms

A	
AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
ACL	Access Control List
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Border Router
B	
BDR	Backup Designated Router
C	
CAR	Committed Access Rate
CLI	Command Line Interface
CoS	Class of Service
D	
DHCP	Dynamic Host Configuration Protocol
DLDP	Device Link Detection Protocol
DR	Designated Router
D-V	Distance Vector Routing Algorithm
E	
EGP	Exterior Gateway Protocol
F	
FTP	File Transfer Protocol
G	
GE	Gigabit Ethernet
H	
HGMP	Huawei Group Management Protocol
I	
IAB	Internet Architecture Board
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
L	
LSA	Link State Advertisement

LSDB	Link State DataBase
M	
MAC	Medium Access Control
MIB	Management Information Base
N	
NBMA	Non Broadcast MultiAccess
NIC	Network Information Center
NMS	Network Management System
NTP	Network Time Protocol
NVRAM	Nonvolatile RAM
O	
OSPF	Open Shortest Path First
P	
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
PoE	Power over Ethernet
Q	
QoS	Quality of Service
R	
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RSTP	Rapid Spanning Tree Protocol
S	
SNMP	Simple Network Management Protocol
SP	Strict Priority
STP	Spanning Tree Protocol
T	
TCP/IP	Transmission Control Protocol/ Internet Protocol
TFTP	Trivial File Transfer Protocol
ToS	Type of Service
TTL	Time To Live
U	
UDP	User Datagram Protocol
V	
VLAN	Virtual LAN
VOD	Video On Demand

VPN	Virtual private network
W	
WRR	Weighted Round Robin
X	
XID	eXchange Identification
XRN	eXpandable Resilient Networking